НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

До захисту допущено:

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інформаційно-комунікаційні технології»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Забезпечення заданих показників безпеки в 5G мережах»

Виконав:
студент IV курсу, групи ТІ-62
Кормульов Олександр Сергійович _____

Керівник:
Доцент кафедри ІТМ, к.т.н, доцент,
Правило Валерій Володимирович _____

Рецензент:
Доцент кафедри ТК, к.т.н, доцент,
Явіся Валерій Сергійович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Лариса ГЛОБА
«___»_____2020 р.

ЗАВДАННЯ

на дипломну роботу студенту
Кормульову Олександру Сергійовичу

1. Тема роботи «Забезпечення заданих показників безпеки в 5G мережах», керівник роботи Правило Валерій Володимирович, кандидат технічних наук, доцент, затверджені наказом по університету від «30» березня 2020 р. № 924-с.

2. Термін подання студентом роботи 8 червня 2020 р.

3. Зміст роботи:

3.1 Аналіз технології 5G та показників безпеки в мережі.
3.2 Аналіз загроз та вразливостей в 5G мережах.
3.3 Забезпечення заданих показників безпеки.

4. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація в PowerPoint

4.1 Тема роботи
4.2 Актуальність
4.3 Об’єкт та предмет дослідження
4.4 Мета та проблема дослідження
4.5 Наукова новизна

4.6 Практична цінність
4.7 Задачі, які виконувались
4.8 Вразливості та загрози в 5G мережах
4.9 Забезпечення безпеки в 5G мережах
4.10 Висновки
4.11 Публікації

5. Дата видачі завдання 09.11.2019

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Отримання та ознайомлення із завданням	09.11.2019 – 20.11.2019	Виконано
2	Огляд особливостей 5G	30.11.2019 – 14.12.2019	Виконано
3	Аналіз роботи 5G, розгляд показників безпеки в мережах 5G.	17.12.2019 – 29.12.2019	Виконано
4	Розгляд та аналіз архітектури безпеки 5G мереж	05.01.2020 – 28.01.2020	Виконано
5	Аналіз вразливостей та загроз в 5G мережах.	04.02.2020 – 17.03.2020	Виконано
6	Представлення вдосконалених методів, написання рекомендацій та пропозицій із забезпечення безпеки в 5G мережах.	03.04.2020 – 29.05.2020	Виконано
7	Оформлення пояснювальної записки про виконану роботу	01.06.2020 – 08.06.2020	Виконано

Студент Олександр КОРМУЛЬОВ

Керівник Валерій ПРАВИЛО

РЕФЕРАТ

Обсяг роботи: робота містить 69 сторінок, 15 рисунків, 1 таблицю, використано 22 джерела.

Актуальність: на відміну від мереж попередніх поколінь, 5G підтримує більше видів послуг та має більш широкий спектр задач, з’являються нові види загроз. Тому виникає питання в забезпеченні безпеки в цих мережах. Тому тема дипломної роботи є актуальною.

Мета роботи: представлення вдосконалених методів, а також рекомендацій та пропозицій із забезпечення безпеки в 5G мережах.

В ході роботи розглянуто загальні поняття 5G та безпеки в цих мережах, проаналізовано архітектуру безпеки 5G мереж, вразливі місця 5G мереж та можливі атаки; проаналізовано існуючі методи забезпечення безпеки, та наведено власні рекомендації та пропозиції по забезпеченню безпеки в 5G мережах.

Публікації:

Правило В.В., Кормульов О.С. Методи забезпечення заданих показників безпеки // Збірник матеріалів XIV Міжнародної науково-технічної конференції "Перспективи телекомунікацій 2020". Київ: 2020. С. 178-180.

Ключові слова: 5G, безпека, мережі, вразливість, загрози.

ABSTRACT

The amount of work: the work contains 69 pages, 15 figures, 1 table and 22 sources have been used.

Topicality: unlike previous generations of networks, 5G supports more types of services and has a wider range of tasks, new types of threats appear. Therefore, there is a question in ensuring security in these networks. Therefore, the topic of the thesis is relevant.

Goal: presentation of improved methods, as well as recommendations and suggestions for security in 5G networks.

During this work the general concepts of 5G and security in these networks are considered, the security architecture of 5G networks, vulnerabilities of 5G networks and possible attacks are analyzed; analyzed the existing methods of security, and mentioned own recommendations and suggestions for security in 5G networks.

Publications:

Pravylo V.V., Kormulov O.S. Methods of ensuring specified security indicators in 5G networks // Proceedings of the XIV International Scientific and Technical Conference "Prospects of Telecommunications 2020". Kyiv 2020. p. 178-180

Keywords: 5G, security, networks, vulnerabilities, threats.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

3GPP	3rd Generation Partnership Project
5G	Fifth Generation
API	Application Programming Interface
ARP	Address Resolution Protocol
CP	Control Plane
C-RAN	Cloud-Radio Access Network
DDoS	Distributed Denial of Service
eMBB	enhanced Mobile Broadband
IMS	Information Management System
IoT	Internet of Things
ITU-R	International Telecom Union Radiocommunication Sector
LTE	Long-Term Evolution
M2M	Machine-to-Machine
MAC	Media Access Control
MEC	Multi-access Edge Computing
MIoT	Massive Internet of Things
mMTC	Massive Machine-Type Communications
OAM	Operations, Administration and Management
RAN	Radio Access Network
SDN	Software-Defined Networking
SIM	Subscriber Identification Module
UE	User Equipment
UICC	Universal Integrated Circuit Card
UP	User Plane
URLLC	Ultra-Reliable Low Latency Communication
V2X	Vehicle-to-Everything
NFV	Network Functions Virtualization

ВСТУП

Актуальність. З швидким розвитком мобільних мереж п'ятого покоління постає питання в забезпеченні безпеки в цих мережах. Незважаючи на те, що в стандарти 5G включені вбудовані функції безпеки, самої по собі мережевої інфраструктури недостатньо для вирішення всіх проблем, пов'язаних з безпекою. На відміну від мереж попередніх поколінь, 5G підтримує більше видів послуг та має більш широкий спектр задач. Такі технології, як пристрої, підключені до Інтернету речей (IoT), доповненої реальності (AR), віртуальної реальності (VR) та інші, вимагають швидкої, надійної та обширної мережі, щоб не відставати від темпів розвитку. Нові підприємства та нові технології, що працюють в епоху 5G, зіткнуться з новими проблемами безпеки та конфіденційності.

Майбутні мережі зв'язку 5G не тільки успадкують уразливості мереж четвертого покоління, а й можуть обзавестися новими недоліками безпеки. Поряд з високою швидкістю (в 10-1000 разів більшою ніж у 4G), низьким енергоспоживанням і мінімальними затримками сигналу, очікується активне використання в мережах 5G технологій віртуалізації мережевих функцій (Network Function Virtualization). Заміна апаратних елементів програмними має багато позитивних ефектів, проте потенційно зробить стільникові мережі ще більш уразливими для атак зловмисників. [1]

Об’єкт дослідження: забезпечення безпеки мереж 5G

Предмет дослідження: 5G мережі

Практична значимість даної роботи полягає в можливості застосування її на практиці при проектуванні та впровадженні 5G мереж, заключає в собі підвищення інформаційного захисту 5G мереж в умовах інформаційних атак, негативного впливу навколишнього середовища, а також фізичного втручання.

Наукова новизна полягає в розробці вдосконалених методів забезпечення безпеки в 5G мережах.

РОЗДІЛ 1.

АНАЛІЗ ТЕХНОЛОГІЇ 5G ТА ПОКАЗНИКІВ БЕЗПЕКИ В МЕРЕЖІ

1.1 Загальні відомості про 5G мережі

5G - це п’яте покоління мобільних мереж, новий етап розвитку технологій, який покликаний розширювати можливості доступу до Інтернету через мережі радіодоступу, пропонує надійніші з'єднання на смартфонах та інших пристроях, ніж будь-коли раніше.

Найбільшою відміною 5G від мереж минулого покоління – більш висока швидкість інтернету. Теоретична можлива швидкість коливається від 10 до 20 Гбіт/с з мінімальними затримками в передачі сигналу (всього 1-2 мс). До прикладу, максимальна теоретична можлива швидкість в 4G складає до 1 Гбіт/с з затримкою сигналу 10 мс, а в 3G – до 42 Мбіт/с з відгуком 100 мс.

Висока швидкість 5G відкриває величезне поле можливостей: нові види послуг, сервісів та цілі бізнес-моделі, які здавалися неможливими в мережах минулих поколінь. До переваг 5G в порівнянні з мережами минулих поколінь можна віднести можливість підключення великої кількості пристроїв, високу енергоефективність, високу мобільність користувачів; в декілька разів зросла пропускна здатність, яка дозволяє забезпечити більшу доступність широкосмугового мобільного зв'язку. Також уваги заслуговує ще одна важлива відміна 5G – віртуалізація. Багато функцій в новій технології реалізовані програмним способом, а не на рівні фізичної інфраструктури, як це було в мережах 4G.

Розробку глобального стандарту, який служить для підготовки до розгортання мереж п’ятого покоління, веде ряд міжнародних організацій, серед яких:

- 3GPP
- ITU-R

В 2015 році почалася робота над 5G, коли організацією ITU-R було визначено стандарт IMT-2020, в якому містяться ключові вимоги до технології нового покоління. У порівнянні з попереднім стандартом IMT-Advanced, який був актуальним для 4G, вони виглядають наступним чином: (Табл.1.1)

Таблиця 1.1

Ключові вимоги до 5G згідно з IMT-2020 в порівнянні з 4G [7]

Параметри	4G	5G
Пікова швидкість завантаження	1 Гбіт/с	20 Гбіт/с
Швидкість завантаження для користувачів	10 Мбіт/с	100 Мбіт/с
Затримка	10 мс	1-2 мс
Максимальна швидкість переміщення без втрати сигналу	350 км/год	500 км/год
Щільність підключення	100 тис. пристроїв/кв.км	1 млн. пристроїв/кв.км
Трафік на одиницю площі	0.1 Мбіт/с/кв.м	10 Мбіт/с/кв.м

В свою чергу, 3GPP взяли на себе розробку технології радіодоступу (Radio Access Technology) нового покоління - 5G New Radio або 5G NR. Організація працює над стандартами і специфікаціями, що визначають майбутній вигляд технології і нового покоління мобільного зв'язку в цілому.

При впровадженні мереж 5G постає проблема в нестачі традиційних частот в спектрі нижче 6 ГГц. Тому необхідно переходити в нові діапазони. В рамках 5G NR виділяються два діапазони:

- Frequency Range 1
- Frequency Range 2

Frequency Range 1 включає в собі традиційні частоти, діапазон sub-6 GHz, тобто нижче 6 ГГц. Частина діапазонів попередніх поколінь будуть передані під потреби 5G завдяки «рефармінгу» частот. Тобто станції, які

використовувались раніше для LTE або, наприклад, для GSM, продовжать функціонувати на тих самих частотах, але тепер будуть передавати дані на основі технологій 5G. Більш досконалі технології кодування дозволять новому поколінню зв'язку бути на 30% ефективніше, ніж LTE, в тому ж діапазоні.

Frequency Range 2 - принципово нові частоти міліметрового діапазону. Вони починаються з позначки в 24 ГГц, піднімаючись приблизно до 50 ГГц і вище в залежності від країни і оператора. Ці частоти мають малу дальність поширення і проникаючу здатність. Їх функціонування забезпечать Small cells - численні малі стільники, а не традиційні базові станції.

Число абонентів в 5G росте в кілька разів швидше, ніж це було в мережах 3G і LTE. Наприклад, в мережах 3G за 10 років з’явилось 500 млн. користувачів. Таке ж число з'явилося за 5 років в мережах 4G. За прогнозами аналітиків, в мережах 5G цей поріг буде досягнутий всього за 3 роки.

Згідно з IMT-2020, існує три базових сценарії використання мобільного зв'язку 5G:

а) eMBB - Enhanced Mobile Broadband / Покращений Мобільний Широкосмуговий зв'язок

б) URLLC - Ultra Reliable and Low Latency Communications / Наднадійна комунікація з низькою затримкою

в) мMTC - massive Machine Type Communication / Масові міжмашинні комунікації

Перший сценарій – це звичайний Інтернет, але більш швидкий і якісний. Швидкість зможе досягати 1 Гбіт/с в приміщеннях, а на вулиці - до 300 Мбіт/с. Граничні швидкості стануть можливі на етапі установки найбільш досконалих антен, що працюють в міліметровому діапазоні (mmWave). Завдяки своїм незначним розмірам, вони вдало впишуться в ландшафт - наприклад, на стовпах, деревах, стінах будівель.

URLLC – це комунікації, в яких важлива не стільки швидкість, скільки низька затримка. Це актуально для автономного транспорту, яким в

критичній ситуації для прийняття рішення може знадобитися менше мілісекунди. В даний час йде дискусія про заміну подібними технологіями супутникової навігації.

Міжмашинні комунікації або M2M, а також IoT - окремий сегмент споживачів зв'язку 5G. Він характеризується підключенням великої кількості пристроїв, найчастіше промислових, з низьким енергоспоживанням, для яких основною вимогою є стабільність та надійність підключення. До них належать вимірювальні пристрої, датчики, сенсори, об'єкти інфраструктури розумного міста.

Для кожного з сценаріїв підходить певний спектр частот і інфраструктура:

– Радіохвилі в діапазоні низьких частот, до 1 ГГц, завдяки своїй проникній здатності добре працюють в закритих приміщеннях. Вони забезпечать роботу систем IoT, розумних будинків, M2M. Також частота 700 МГц може використовуватися для забезпечення зв'язком віддалених населених пунктів.

– Середній спектр або mid-band frequencies (від 1 до 6 ГГц) поєднує в собі оптимальну ємність і покриття для первинного впровадження eMBB, а далі - URLLC і mMTC.

– Міліметрові хвилі (> 24 ГГц) реалізують всю повноту можливостей 5G. Пріоритетна сфера застосування - високонавантажені зони трафіку (хот-споти), масові скупчення користувачів.

– Release 16, що розробляється 3GPP, доповнить цей перелік новими сценаріями, серед яких:

– V2X (Vehicle-to-Everything) - передача даних з низькою затримкою між рухомими безпілотними транспортними засобами і хмарними дата-центрами для віддаленого управління і обслуговування.

– Satellite access - супутниковий доступ.

Як і будь яка нова технологія, 5G несе в собі ризики. Основними загрозами можна вважати:

а) Перетин частот

Незважаючи на планований «рефармінг», багато спектрів частот все ще експлуатуються спеціальними службами та установами, серед яких наукові лабораторії, космічні та військові відомства. Виділення діапазонів для комерційного використання потребують ретельного всебічного узгодження.

б) Кібератаки

Інтернет речей, який напряму пов’язаний з 5G, схильний до атак точно так же, як і усі електронні пристрої. Користувачі повинні будуть подбати про забезпечення безпеки своїх пристроїв, а компанії і державні органи - зробити серйозні зусилля для забезпечення захисту розумних міст і Industrial IoT.

1.2 Поняття безпеки в 5G

Безпека в 5G - це захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести до нанесення шкоди власникам або користувачам інформації і підтримуючої інфраструктури.

Поняття безпеки в 5G, як і захист інформації, завдання комплексне, спрямоване на забезпечення безпеки, що реалізується впровадженням системи безпеки. Проблема захисту інформації є багатоплановою і комплексною і охоплює ряд важливих завдань.

Основними загрозами в 5G мережах є:

– Загрози пов'язані з навколишнім середовищем (стихійні лиха, техногенні катастрофи і т.д.);

– Технічні (відмови обладнання і програмного забезпечення, витік інформації по каналах зв'язку і т.д.);

– Людські (в результаті навмисних і ненавмисних дій).

Як і будь-яка масштабна технологія, 5G приверне увагу хакерів і кіберзлочинців.

Концепція безпеки мереж 5 п'ятого покоління включає в себе:

- Автентифікацію користувача з боку мережі.

- Автентифікацію мережі з боку користувача.
- Узгодження криптографічних ключів між мережею і призначеним для користувача обладнанням.
- Шифрування і контроль цілісності сигнального трафіку.
- Шифрування і контроль цілісності призначеного для користувача трафіку.
- Захист ідентифікатора користувача.
- Захист інтерфейсів між різними елементами мережі відповідно до концепції мережевого домену безпеки.
- Ізоляцію різних верств механізму network slicing і визначення для кожного шару власних рівнів безпеки.
- Автентифікацію користувача і захист трафіку на рівні кінцевих сервісів (IMS, IoT та інших).

Безпека телекомунікаційних мереж визначається такими компонентами:

- Стандартизація; процес, згідно з яким оператори, постачальники та інші зацікавлені сторони встановлюють стандарти для того, як мережі працюватимуть разом по всьому світу. Сюди також входить, те як найкраще захистити мережі та користувачів від зловмисників
- Дизайн мережі; постачальники мереж конструюють, розробляють та реалізовують узгоджені стандарти для функціональних мережевих елементів та систем, які відіграють вирішальну роль у створенні кінцевого мережевого продукту як функціональним, так і безпечним
- Конфігурація мережі; на етапі розгортання, мережі налаштовуються на цільовий рівень безпеки, що є ключовим для встановлення параметрів безпеки та подальшого посилення безпеки та стійкості мережі

- Розгортання та експлуатація мережі; операційні процеси, які дозволяють мережам функціонувати та забезпечувати цільовий рівень безпеки, сильно залежать від розгортання та роботи самої мережі

Стандартизація відіграє важливу роль з початку появи глобальних стільникових мереж, таких як GSM або 2G. У цьому процесі оператори та постачальники домовляються про те, як мережі працюватимуть разом у всьому світі і як мережі та користувачі можуть бути захищені від зловмисних учасників. Постачальники мережі перекладають узгоджені стандарти на функціональні мережеві елементи та системи. Проектування та розробка, що виконуються постачальником мережі, є ключовою частиною того, щоб кінцевий мережевий продукт вийшов функціональним та безпечним.

На етапі розгортання, мережі також розробляються та налаштовуються для цільового рівня безпеки, а також встановлюються параметри безпеки та додатково посилюється стійкість мережі. На етапі експлуатації, операційні процеси, які полегшують мережу та забезпечують цільовий рівень безпеки, сильно залежать від розгортання та роботи мережі. Один із способів зображення цих чотирьох взаємопов'язаних процесів показаний на рис 1.1.

Високий рівень забезпечення безпеки продукту є життєво важливим для успіху в галузі безпеки. Забезпечення безпеки - важливий процес при розробці програмного забезпечення постачальника, як правило, містить набір підпроцесів на різних рівнях для забезпечення того, щоб продукт функціонував та працював так, як було призначено. До прикладів таких підпроцесів можна віднести оцінку вразливості, тестування на проникність, чи оцінку ризику та оцінку впливу на конфіденційність. Крім того, кожен фрагмент коду потрібно переглянути та відсканувати на предмет недоліків та вразливостей. Забезпечення безпеки не обмежується лише внутрішньою діяльністю.

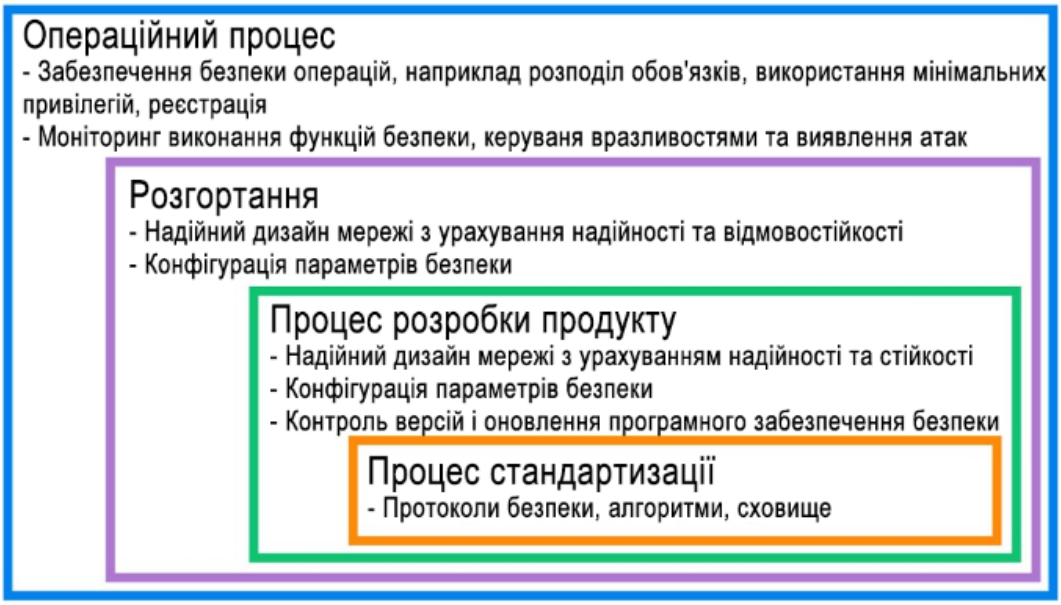

Рис 1.1 Розгляд ключів безпеки [10]

1.3 Архітектура безпеки в 5G

Архітектура безпеки 5G - сукупність механізмів і процедур безпеки, реалізованих в мережах 5-го покоління, які охоплюють всі компоненти мережі, починаючи від ядра і закінчуючи радіоінтерфейсом.

Одним з ключових моментів при створенні безпечних систем є використання архітектури безпеки. Наявність такої архітектури дає можливість детально розглянути всі об'єкти, пов'язані з системою, і їх взаємовідносини. Подібна комплексна оцінка дозволяє проаналізувати рівень безпеки системи в цілому і безпеку її окремих частин, зрозуміти, як ці частини впливають на систему, виявити можливі загрози і розробити ефективні заходи протидії їм і управління безпекою.

Мережі 5 п'ятого покоління є, по суті своїй, еволюцією мереж 4-го покоління LTE. Ядро мережі не зазнало значних змін, на відміну від технологій радіодоступу. Тому, архітектура безпеки 5G-мереж була розроблена з упором на перевикористання відповідних технологій, прийнятих в стандарті 4G LTE.

Проте, переосмислення таких відомих загроз, як атаки на радіоінтерфейси і рівень сигналізації (signalling plane), DDOS-атаки, Man-In-

The-Middle атаки і ін., спонукає операторів зв'язку розробити нові стандарти і інтегрувати абсолютно нові механізми безпеки в мережі 5 п'ятого покоління.

Ключовими принципами архітектури мереж 5G є:

- Поділ мережевих вузлів на елементи, що забезпечують роботу протоколів площини користувачів (UP - User Plane) і елементи, що забезпечують роботу протоколів площини управління (CP - Control Plane), що підвищує гнучкість в частині масштабування і розгортання мережі, тобто можливе централізоване або децентралізоване розміщення окремих складових мережевих вузлів.
- Підтримка механізму network slicing, грунтуючись на послуги, що надаються конкретним групам кінцевих користувачів.
- Реалізація мережевих елементів у вигляді віртуальних мережевих функцій.
- Підтримка одночасного доступу до централізованих і локальних служб, тобто реалізація концепцій хмарних (Fog computing) і граничних (Edge computing) обчислень.
- Реалізація конвергентної архітектури, що об'єднує різні типи мереж доступу - 3GPP 5G New Radio і non-3GPP (Wi-Fi і т. п.) - з єдиним ядром мережі.
- Підтримка єдиних алгоритмів і процедур аутентифікації незалежно від типу мережі доступу.
- Підтримка мережевих функцій без збереження їх стану (Stateless), в яких обчислюється ресурс відділений від сховища ресурсів.
- Підтримка роумінгу з маршрутизацією трафіку як через домашню мережу, так і в гостьовій мережі.
- Взаємодія між мережевими функціями представлена двома способами: сервісно-орієнтована і інтерфейсна.

Основними складовими архітектури безпеки є домени, шари, сфери безпеки і класи управління безпекою.

Домен - це група мережевих об'єктів, відібрана відповідно до визначених фізичними або логічними параметрами, важливими для конкретної мережі 5G.

Шар (рівень) - це протоколи, дані і функції, пов'язані з якимось аспектом послуг, що надаються одним або декількома доменами.

Сфера безпеки (SR) охоплює всі потреби безпеки одного або декількох шарів / доменів.

Класи управління безпекою (SCC) - сукупність функцій і механізмів захисту системи (включаючи заходи і контрзаходи), які стосуються якогось одного аспекту безпеки, наприклад, забезпечення цілісності даних. SCC допомагають уникати, виявляти, стримувати, протидіяти або мінімізувати ризики безпеки в мережах 5G, включаючи погрози фізичної і логічної інфраструктурі мережі, призначеному для користувача устаткування і безпеки переданих даних.

Домени дозволяють легко описати різні функції і учасників в мережах 5G. На рис 1.2. зображені основні домени 5G і показано їх розташування в мережі. Горизонтальні лінії H1, H2 і вертикальні лінії V1, V2 поділяють домени верхнього рівня. Ті домени, що розташовані вище H1, являють собою різні компоненти логічної мережі і називаються доменами учасників; домени між H1 і H2 відповідають за фізичні компоненти мережі і називаються інфраструктурними доменами; домени, які знаходяться нижче H2 - це складові домени, що відповідають відразу за кілька аспектів мережі, наприклад, за належність чи спільне адміністрування. V1 відокремлює призначене для користувача устаткування від мережевого, а V2 відокремлює мережу оператора від зовнішньої мережі, наприклад, від Інтернет-сервісів.

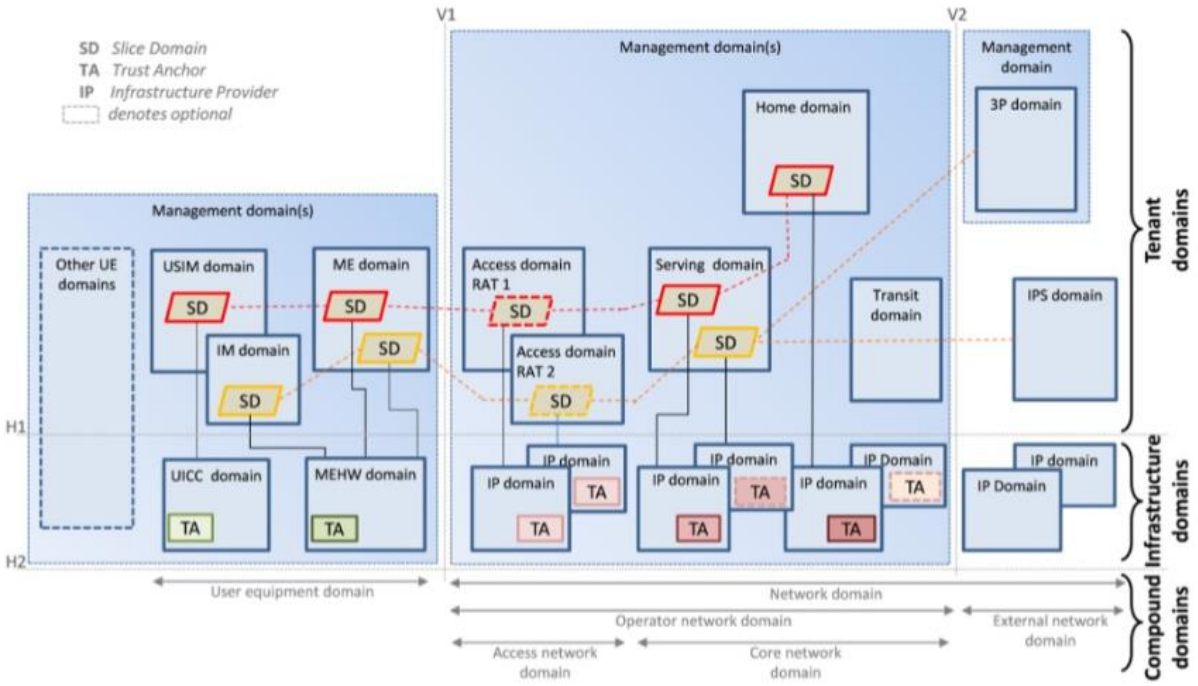

Рис. 1.2 Архітектура безпеки 5G мереж: SD - мережеві слайси, TA - якір довіри, IP - постачальник інфраструктури [11]

На рис. 1.3. показана схема шарів в архітектурі безпеки мереж 5G. Вони об'єднані за принципом загальних вимог до безпеки і схильності одним і тим же типам загроз, наприклад, підміні базових станцій на фейкові (фальшиві) або створення перешкод радіосигналу - це загальні загрози для призначеного користувацького устаткування і точок доступу, з якими воно взаємодіє. Використання шарів допомагає краще структурувати системи управління безпекою в мережах 5G і визначити, де і для яких цілей їх більш ефективно використовувати.

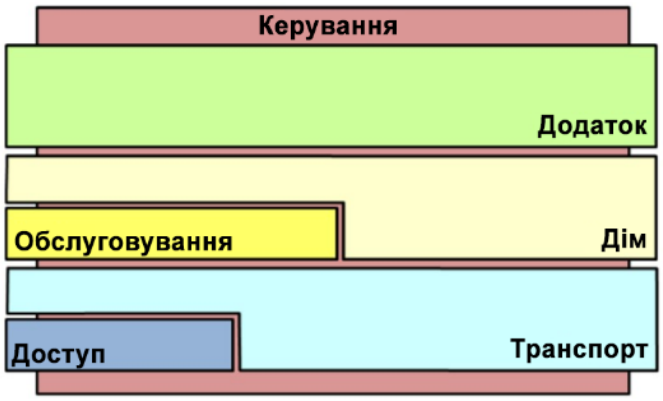

Рис. 1.3 Шари (рівні) в архітектурі 5G [11]

В ці шари входять протоколи і функції, пов'язані, наприклад, з обслуговуванням кінцевих користувачів; обробкою і зберіганням даних про передплату та послуги для домашніх мереж; наданням телекомунікаційних послуг; передачею даних користувачів з інших шарів через мережу.

Коли користувачі перебувають в роумінгу, частина протоколів і функцій шару «Дім» бере на себе шар «Обслуговування», який вважається його підшаром. Аналогічно, шар «Доступ» є підшаром для «Транспорт», так як радіоінтерфейс - це частина загальної системи передачі даних. Шар «Управління» відображає загрози, до яких схильні системи управління в мережах 5G, наприклад, несанкціоновані зміни конфігурації, компрометація мережевих ключів і сертифікатів і додавання шкідливих мережевих функцій. Він знаходиться за іншими верствами на схемі, так як відповідає за управління мережевими функціями всіх шарів системи.

Сфери безпеки застосовуються в архітектурі для опису потреб і вимог до безпеки в певних областях, тому їх склад відрізняється в залежності від конкретної ділянки і функціональності мережі. Наприклад, для сфери безпеки доступу до мережі, важливі захист систем зберігання даних на базових станціях, захист від несанкціонованого впровадження даних по повітрю, захист від переадресації та підключення абонентів до фальшивих базових станцій. У той же час для сфери базової безпеки мережі головними факторами є захист конфіденційності ідентифікаторів, безпечна автентифікація і авторизація, безпека поширення ключів і обміну алгоритмами.

Основні класи управління безпекою - це управління ідентифікацією та доступом, автентифікація, відмовостійкість, конфіденційність, цілісність, доступність і приватність інформації, а також аудит, довіра і гарантії, і відповідність вимогам. Механізми захисту, засновані на класах управління безпекою - це, наприклад, надання довгострокових (IMSI в 3GPP) і короткострокових (TMSI або GUTI в 3GPP) ідентифікаторів для управління ідентифікацією і доступом; AKA в 3GPP і HTTP Digest для автентифікації

користувачів або використання асиметричної криптографії та цифрових підписів для забезпечення відмовостійкості.

1.3.1 Аналіз системи та впровадження архітектури безпеки

Методика аналізу системи і впровадження архітектури безпеки виглядає наступним чином:

1. Необхідно створити модель мережі 5G, почавши з фізичних і логічних доменів верхнього рівня. Головними їх характеристиками стануть належність, управління і призначення. Потім необхідно виділити типи мережевих слайсів (slice domains), які будуть підтримуватися системою. Ця доменна модель верхнього рівня повинна ґрунтуватися на функціональній архітектурі самої мережі.

2. Далі необхідно ввести контрольні точки (інтерфейси), що зв'язують певні домени. Ці контрольні точки будуть визначати залежності та тип взаємодії між доменами. Дані, які передаються через ці точки, необхідно ідентифікувати і описати згідно з обраними шарами і протоколами, потім призначити для них відповідні сфери безпеки.

3. Для кожної контрольної точки необхідно визначити тип взаємин і ступінь «довіри» між пов'язаними доменами.

4. Наступним пунктом стане проведення Threat, Vulnerability And Risk Assessment (TVRA) - оцінки загроз та ризиків, і складання плану боротьби з ними за допомогою класів управління безпекою. Одним з проміжних кроків в TVRA обов'язково повинно стати визначення того, де і ким будуть вживатися заходи щодо забезпечення безпеки, а при аналізі необхідно враховувати використовувані в системі домени, шари і сфери безпеки.

5. Вибір класів управління безпекою повинен ґрунтуватися на принципах security-by-design, тобто програмне забезпечення було розроблено з основою для забезпечення безпеки, і використовувати найбільш ефективні та перевірені методи забезпечення безпеки.

6. Необхідно впровадити обрані заходи безпеки і зробити перевірку того, чи були в результаті досягнуті цілі і задачі, які ставились на початку.

1.3.2 Показники ефективності архітектури безпеки 5G-мережі

До показників, які допоможуть визначити ефективність створеної архітектури безпеки мережі 5G, відносяться:

- Зворотна сумісність: можливість використовувати архітектуру безпеки мережі 5G для опису і аналізу безпеки мереж 3G і 4G, оскільки вони стануть невід'ємною частиною мереж нового покоління.
- Гнучкість і адаптивність: можливість адаптувати архітектуру безпеки до мережевих рішень. Також мова йде про можливості розвитку і вдосконалення архітектури безпеки, щоб ефективно протидіяти новим загрозам і забезпечити сумісність з новими системами безпеки, яких не було на момент її розробки.
- Питання довіри: мобільні мережі четвертого покоління припускають тристоронню модель довіри за участю мобільного оператора, постачальника послуг і кінцевого користувача, де за стан і безпеку мережі відповідає оператор мобільного зв'язку. Ця модель не підходить для мереж 5G, в яких з'явиться набагато більше учасників з різними ролями, наприклад, постачальники віртуалізованої інфраструктури або постачальники VNF (віртуалізовані мережеві функції), і для кожного з них необхідно чітко прописати роль в новій багатосторонній моделі довіри.
- Віртуалізація та «слайсінг» або нарізка мереж: очікується, що мережі 5G будуть підходити для абсолютно будь-якого сценарію використання. Оскільки різні варіанти їх використання висувають до цих мереж абсолютно різні вимоги, які можуть навіть суперечити один одному, мережі 5G повинні бути універсальними. І в цьому їм допоможуть технології віртуалізації і Network Slicing (нарізка мереж). Тому віртуалізація і слайсінг також повинні стати обов'язковою частиною архітектури безпеки 5G.

- Протоколи і мережеві функції: як уже було з мобільними мережами поточного покоління, разом з впровадженням 5G з'явиться ряд нових (як захищених, так і незахищених) протоколів і мережевих функцій. При цьому для нормальної роботи мереж 5G буде використовуватися їх величезна кількість, включаючи і успадковані від попередніх поколінь рішення. Тому архітектура безпеки повинна вміти ідентифікувати всі застосовувані протоколи і мережеві функції для розробки найбільш ефективної системи захисту.
- Точки управління безпекою: мережі 5G будуть набагато складніше, ніж мережі 4G і більш ранніх поколінь. У них буде набагато більше учасників, більше різних рівнів і засобів доступу до мережі. Крім цього, мережі 5G будуть більш динамічними в тому сенсі, що нові (віртуалізовані) мережеві вузли зможуть автоматично додаватися і віддалятися з мережі або її частини практично в будь-який момент. Чітке визначення меж та інтерфейсів мережі вкрай важливо для ідентифікації та моделювання векторів атак.
- Управління безпекою: Поряд з новими сценаріями використання, новими моделями довірчих відносин і новими технологіями, які принесуть із собою мережі 5G, з'являться нові функції безпеки і нові проблеми. Тому архітектура безпеки повинна враховувати це і дозволяти моделювати мобільні мережі з різним набором функцій і різними слабкими місцями.
- Управління мережею: специфікації четвертого покоління мобільних мереж ніяк не формалізують аспекти управління мережею, так як вважається що це залежить від реалізації і сценаріїв застосування конкретних мереж. У мережах 5G з'являться нові ролі і нові учасники, тому питання управління мережею важливі для забезпечення ефективного і безпечного її функціонування, і це повинно бути відображено в архітектурі безпеки.

Висновки до розділу: в першому розділі проаналізовано роботу 5G мереж, розглянуто поняття і проблему безпеки, розглянуто архітектуру безпеки мереж 5G, проведено аналіз системи і алгоритму впровадження

архітектури безпеки. Також проведена оцінка показників ефективності архітектури безпеки.

Незважаючи на те, що архітектура безпеки 5G базується на перевикористанні існуючих технологій, перед нею ставляться зовсім нові завдання. Величезна кількість IoT-пристроїв, розширені межі мережі і елементи децентралізованої архітектури - ключові принципи стандарту 5G, в яких в майбутньому з’являться вразливі місця та виникнуть нові загрози, які й підіймуть питання безпеки в 5G-мережах.

РОЗДІЛ 2.

АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ В 5G МЕРЕЖАХ

2.1 Загрози 5G пов’язані з Інтернетом речей

З розвитком мереж п'ятого покоління буде стрімко збільшуватися кількість експлуатованих абонентських і IoT-пристроїв. А масове поширення таких пристроїв, які не мають функцій безпеки, відкриває широкі можливості для хакерів і створює величезні проблеми для безпеки організацій. Ситуацію ускладнює масштаб: в найближчі декілька років підприємства можуть підключити до мережі мільярди пристроїв. Результатом злому IoT може стати зараження таких пристроїв для створення ботнетів і проведення масових DDoS-атак об'ємом 1 Тб/с і вище.

У 2016 році хакери запустили одні з найбільших кібератак в історії Інтернету. Ці DDoS-атаки були виконані шляхом зараження декількох підключених до Інтернету пристроїв (наприклад, камер спостереження, відеореєстраторів, маршрутизаторів), а потім їх використовували для запуску скоординованих DDoS-атак на масив цілей, включаючи провайдерів та журналістів. Атаки називались вірусом Mirai. Тривожним фактом про Mirai, який з'ясувався пізніше, коли було розкрито вихідний код, була відносна відсутність вишуканості програмного забезпечення. Запуск цього ботнету не вимагав високих навичок програмування. Основні інструменти легко доступні та знаходяться в вільному розпорядженні в Інтернеті. Подія з Mirai дозволила виділити ключові проблеми з безпекою в Інтернеті речей.

Існує чотири загальних принципа, які заслуговують на увагу для забезпечення безпеки інфраструктури IoT:

1. Питання забезпечення безпеки IoT не повинно вирішуватися в останню чергу. Питання безпеки IoT потрібно вирішувати на етапі проектування, а не додавати його після розгортання.

2. IoT по своїй суті включає в собі кілька рівнів безпеки: апаратна безпека, безпека програмного забезпечення, безпека даних, сховища, мережі,

додатків, та ін. Взаємозв'язок між цими рівнями дуже важливий. Загальна конструкція безпеки IoT повинна враховувати цей факт.

3. Безпека IoT сильно залежить від її найменших елементів. Найчастіше, значна увага приділяється забезпеченню безпеки мобільного телефону, ігноруючи при цьому, здавалось би, незначні елементи, такі як спринклер або додаток який імітує ключі від автомобілю (CarKey). Проблеми з безпекою в таких елементах можуть привести до глобальних атак на IoT та 5G

4. Комплексні пристрої IoT (наприклад, промислове обладнання, підключені автомобілі) - найскладніші середовища для IoT. Також наслідки від, наприклад, зламаного підключеного автомобіля, можуть бути значно серйознішими порівняно з наслідками підключеного електролічильника або холодильника.

Повна безпека IoT повинна враховувати безпеку на багатьох рівнях, як показано на рис 2.1.. На сьогодні пристрої та мережа/транспорт можуть бути основними в центрі уваги, але з точки зору прибутків ключовими є платформи, додатки та послуги.

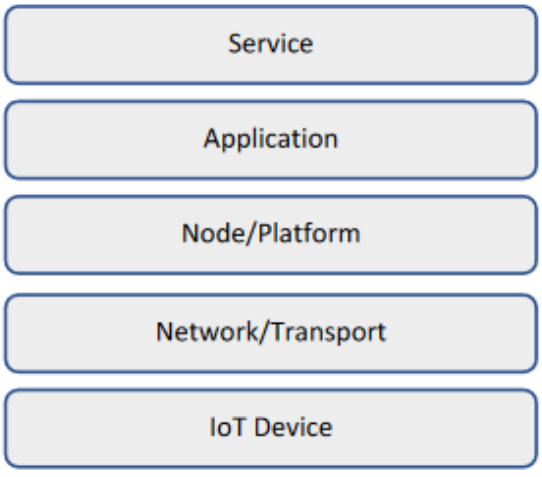

Рис. 2.1 Рівні безпеки в IoT [16]

IoT Device (пристрій IoT) - багато пристроїв IoT, скоріш за все, перебувають у відкритих незахищених та вразливих умовах. Дані пристроїв

користувачів можуть бути підроблені. Шкідливі оновлення вбудованого програмного забезпечення пристрою та ОС створюють значну проблему.

Network/Transport (Мережа/Транспорт) – мережеве з'єднання дозволяє забезпечити безпечну взаємодію пристроїв/додатків із обслуговуючими мережевими вузлами. Для забезпечення цієї взаємодії необхідна безпечна ідентифікація/автентифікація та транспортування даних. Мережеве з'єднання в IoT повинно ефективно обробляти мільярди пристроїв.

Node/Platform (Вузол/Платформа) – платформи IoT повинні забезпечувати безпеку даних та команд керування. Крім того, платформи також відповідають за забезпечення ізоляції між пристроями та користувачами та сторонніми додатками та службами.

Applications (додатки) - додатки можуть розглядатися як комбінація багатьох мікросервісів, що використовуються для створення одного сервісу. Ці програми можуть статично розміщуватися або динамічно переноситися в середовище, яке є оптимальним для їх реалізації. Захист програм буде результатом самого коду програми та платформи, яку він використовує. У випадках, коли додатки можуть переноситися, важливо, щоб міграція між платформами відбувалася безпечно.

Service (сервіс) – завдяки IoT з'являється безліч нових служб. Новою ключовою послугою, в якій IoT буде відігравати значну роль і де забезпечення безпеки є першорядним, - це підключені автомобілі. Для великих груп підключених транспортних засобів, які рухаються з високою швидкістю, безпека завжди залишатиметься в центрі уваги. Якщо втрачено з'єднання з мережею через несправності, або заклинювання, необхідні резервні механізми, на яких робота служба може відновитися. Існує багато інших сервісів різної степені критичності, які можуть бути включені IoT. Шлях до забезпечення безпеки різних служб IoT повинен враховувати їх унікальність, а також критичність самого сервісу.

2.2 Загрози пов’язані з Massive IoT

Massive IoT (MIoT) охоплює широкий спектр нових широких можливостей, таких як автономна комунікація транспортних засобів, розумні мережі електропостачання, датчики руху/трафіку, комунікації за допомогою дронів, медичні датчики та AR/VR. Риночна можливість MIoT, його унікальні вимоги та міркування кібербезпеки безпосередньо впливають на архітектуру 5G. Два приклади - використання граничних обчислень мультисервісного доступу в 5G та підтримка надійних комунікацій з низькою затримкою (URLLC).

Рис. 2.2. ілюструє сценарій коли хакери експлуатують вразливість нульового дня (zero-day) у пристроях MIoT для запуску DDoS-атак на 5G RAN. Хакери можуть бути простими людьми, які просто хочуть порушити мобільну мережу, або вони можуть бути державою, яка атакує всіх мобільних операторів в іншій країні.

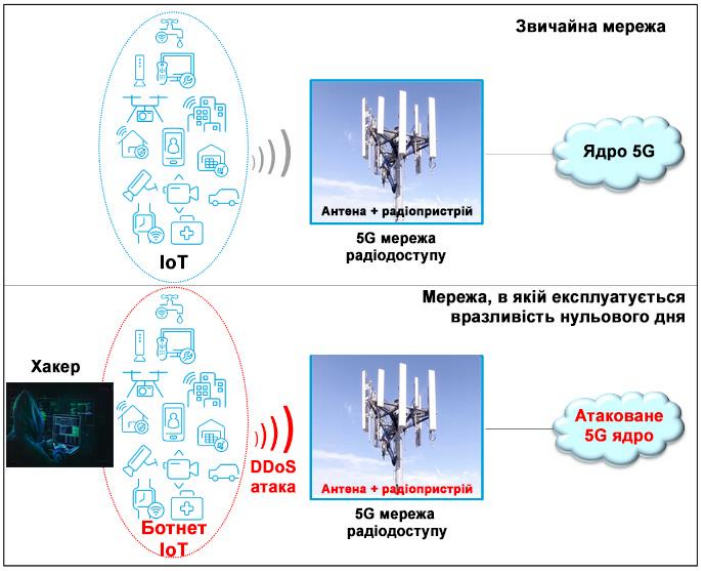

Рис. 2.2 Хакерські атаки з експлуатацією вразливостей нульового дня

На Рис. 2.3 представлені загрози 5G. Різні суб'єкти та сегменти 5G, такі як UE (User Equipment), RAN (Radio Access Network), базова мережа та додатки і сервіси операторів або сторонніх осіб, можуть бути мішенню різних суб'єктів загроз. Наприклад, хактивісти, організовані злочинні угрупування, можуть запускати кібератаки на 5G мережі з метою

компрометації інформації, шахрайства, крадіжок ідентифікаторів користувачів, заподіяння шкоди репутації брендам або роблять недоступними мережеві функції та сервіси 5G.

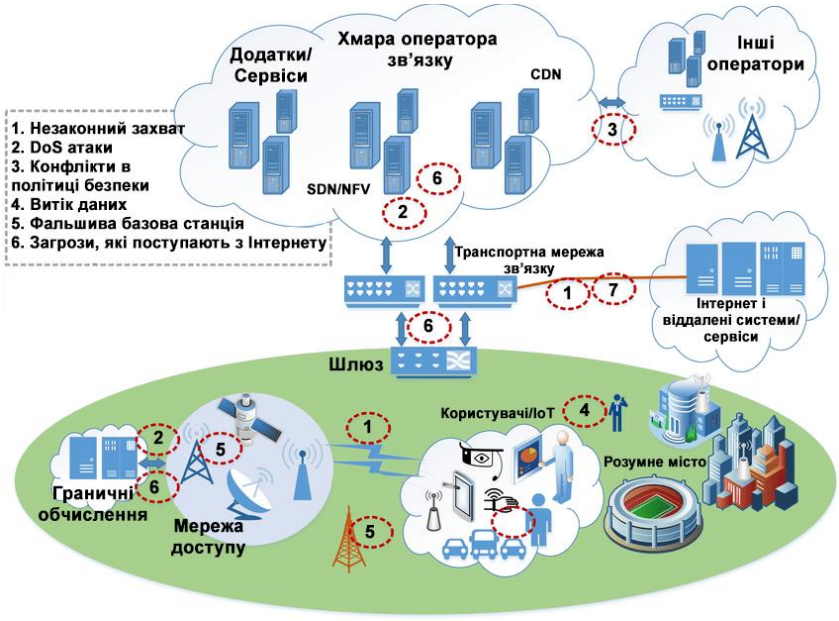

Рис. 2.3 Загрози в 5G [15]

2.3 Загрози опорної мережі

До загроз які виникають в опорних (базових) мережах можна віднести:

Неправомірне використання віддаленого доступу: ця загроза полягає у тому, що зловмисник опановує віддаленим доступом до критичних мережевих компонентів та бере під контроль віртуальну машину для виконання різних типів атак. Віддалений доступ - це стандартна практика в галузі індустрії технологій для полегшення обслуговування та експлуатаційних процедур. Отримавши незаконний доступ до функції віддаленого доступу, зловмисник може підключитися до операційних систем та додатків в критично можливому домені мережі. Маючи доступ до віртуальної машини в мережі, злочинець може займатися іншими зловмисними діями, такими як підробка даних конфігурації та розповсюдження зловмисного програмного забезпечення.

Неправомірне використання даних автентифікації/даних авторизації. Ця загроза пов'язана з розкриттям довгострокових ключів для автентифікації

та контролю безпеки, що проводяться інсайдерським або ворожим чи недовіреним персоналом, який працює в базовій мережі.

Неправомірне використання сторонніх мережевих функцій: ця загроза стосується питань доступності та розкриття конфіденційних даних через основні функції мережі, які розміщені в системах сторонніх постачальників хмарних послуг. Недостовірний постачальник хмарних послуг може отримати доступ, перервати та змінювати трафік.

Неправомірне використання функції законного перехоплення (Lawful interception): ця загроза розглядає несанкціонований доступ до цієї функції при розміщенні за межами мережі оператора. Якщо вендор/постачальник послуг має доступ до мобільної мережі, він зможе маніпулювати цією функцією та обходити механізми безпеки таким чином, щоб зловживання не було виявлене.

Експлуатація інтерфейсу прикладного програмування (API): ця загроза передбачає використання API для запуску різних типів атак. Значна частина відкритості та програмованості, запропонована новою мережевою архітектурою 5G, покладається на широке використання API. Експлуатація може орієнтуватися на різні типи функцій внутрішньої мережі, Інтернет інтерфейсів, роумінгових інтерфейсів тощо. Неправильно розроблений або налаштований API з неточними правилами контролю доступу може зробити функції базової мережі більш вразливими та чутливими. Загроза наявності одного невеликого компрометованого API в ядрі 5G може поставити під загрозу всю мережу.

Експлуатація погано розробленої архітектури та неналежна адаптація (мережі, сервісів та безпеки): загроза стосується питань, що виникають із безлічі варіантів та особливостей, які ця технологія може запропонувати від свого первісного створення до реалізації. Рівень складності та труднощі досягнення оптимальної архітектури, належної безпеки та експлуатаційних процедур можуть призвести до поганого проектування та впровадження. Недоліки дизайну відкривають перед зловмисниками можливості для

незаконних дій. Знаючи, що певна функція, яка реалізована або захищена не належним чином, хакер може експлуатувати порушення в дизайні та вводити зловмисне програмне забезпечення в основну мережу.

Експлуатація неправильно налаштованих або погано налаштованих систем/мереж: часто ідентифікується як вразливість, це експлуатація неправильно налаштованих або погано налаштованих систем, що кваліфікується як загроза. Експлуатація неправильно сконфігурованої системи, яка по суті має ненавмисний характер, створює можливість хакеру знайти слабкі місця в мережі та здійснити атаку. Недоліки конфігурації можуть траплятися на різних етапах проектування мережі. Приклади включають погано або неправильно налаштовані API, мережеві функції, правила контролю доступу, віртуалізовані середовища, граничні вузли, програмне забезпечення, брандмауери тощо.

Помилкове використання або адміністрування мережі, систем та пристроїв: класифіковано як ненавмисне пошкодження (помилкове адміністрування пристроїв та систем) помилки, спричинені погано підтримуваною та адмініструваною мережею, можуть порушити конфіденційність, цілісність та доступність мережі. Приклад дій, пов’язаних із погано керованою системою, включає відсутність оперативних процесів та процедур, які могли б піддати мережу нападу.

«Вишкрібання» або витягнення (scraping) пам’яті: ця загроза виникає, коли зловмисник сканує фізичну пам’ять програмного компонента, щоб дістати конфіденційну інформацію, яку він не має права отримувати. Хоч і витягування пам'яті може впливати на компоненти будь-якого рівня мережі, цей тип загрози в основному був визначений для серверів додатків SDN. Крім того, для конфігурації SDN можуть знадобитися перезавантаження, які зловмисник може використовувати для атаки на процедуру завантаження. Після успішного виконання, витягування пам’яті може використовуватися для отримання чутливих даних SDN.

Аналізатор трафіку, або «сніффер» - популярний метод, який застосовується зловмисними суб’єктами для збору та аналізу інформації мережевої комунікації. Аналізуючи трафік, зловмисник також може прослуховувати дані з мережевих елементів або посилань та викрасти цінну інформацію. Аналізування трафіку може відбутися в будь-якому місці, де є постійний трафік. Наприклад, у SDN, зловмисник може скористатися незашифрованими повідомленнями для перехоплення трафіку з центрального контролера. Захоплені дані можуть включати критичну інформацію про потоки або трафік, дозволені в мережі.

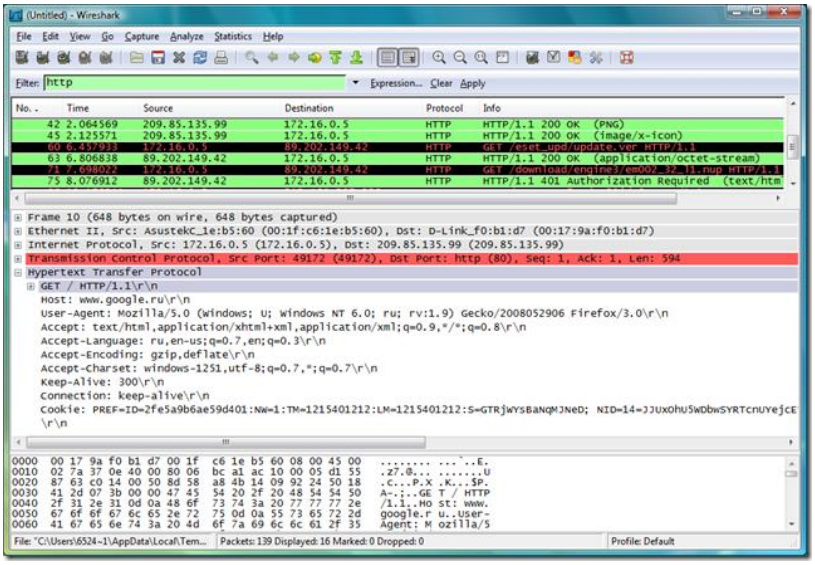

Рис. 2.4 Приклад аналізатору трафіку (сніферу)

Маніпулювання мережевим трафіком, розвідка мережі та збирання інформації: загроза включає зміни чи фальсифікацію даних під час транзиту (повідомлень), введення нелегітимних даних у мережу, чи то шляхом відтворення попередніх повідомлень, чи підробкою нових повідомлень, зміна пріоритетів потоку.

Маніпулювання даними конфігурації мережі: неадекватна політика управління та захисту важливих даних конфігурації може призвести до непередбачуваної поведінки системи та несанкціонованого доступу до критичних платформ, що вплине на конфіденційність та цілісність мережі. Ця загроза передбачає компрометацію основного мережевого елемента (наприклад, контролера SDN, функцій мережі, функцій управління) шляхом

підроблення конфігурації даних для запуску інших атак (наприклад, DoS). Хоч і підробка даних конфігурації, в принципі, може стосуватися даних, що зберігаються будь-яким компонентом мережі, ця загроза стосується конкретно даних конфігурації. Приклади маніпулювання даними конфігурації наведені нижче.

- Маніпулювання таблицями маршрутизації
- Фальсифікація даних конфігурації
- DNS-маніпуляція

Зловмисний флуд компонентів основної мережі: ця загроза передбачає флуд запитами або трафіком, що шкодить доступності мережевого компонента. Флудінг може відбуватися під час передачі даних, виснаження компонентних ресурсів і призводить до скорочення або повного відключення послуги, що надається компонентом.

Зловмисне перенаправлення трафіку: ця загроза передбачає компрометацію мережевих елементів для перенаправлення потоків трафіку та дозволення зловмисному суб'єкту прослуховувати мережевий трафік.

Шахрайські використання спільних ресурсів. Ця загроза стосується несанкціонованого доступу та/ бо модифікації критичних даних підключених пристроїв 5G. Кінцеві ключі можуть бути викрадені або просочені з централізованих ключових серверів. Як наслідок, захищена комунікація стає вразливою для різних атак, а злочинці отримують доступ до кінцевих точок.

2.4 Загрози мережевого доступу

«Отруєння» протоколу визначення адреси (ARP): Цей тип атаки також називається «спуфінгом» (підміною) кешу ARP: техніка, за допомогою якої зловмисник надсилає в мережу підроблені повідомлення ARP. Як правило, мета полягає в тому, щоб зв'язати MAC-адресу зловмисника з IP-адресою іншого хоста, такого як шлюз за замовчуванням, внаслідок чого будь-який трафік, призначений для цієї IP-адреси, буде надісланий хакеру.

Підроблений вузол мережевого доступу: загроза передбачає фальсифікацію зв'язку між абонентським обладнанням та мережею, щоб ініціювати інші шкідливі дії.

Флуд атака: ця загроза передбачає флудінг радіоінтерфейсів запитами. Флуд відбувається за допомогою передачі даних, що може вичерпати ресурси компонентів і призвести до скорочення або повного відключення радіочастоти.

Заглушка радіочастоти: ця загроза класифікується як шкідлива діяльність, що полягає у навмисному перебої мережевої радіочастоти (NRF), внаслідок чого основна мережа (та пов'язані з нею послуги) стають недоступними для користувачів. Загроза також стосується втручання в систему геопозиціонування (GPS).

MAC-spoofing (спуфінг, підроблення): метод зміни MAC адреси на мережевому пристрої. Полягає в тому, що на мережевій карті змінюється MAC-адреса, що змушує комутатор відправляти на порт, до якого підключений зловмисник, пакети, які до цього він бачити не міг. MAC-Spoofing зображено на рис. 2.5.

Маніпулювання даними конфігурації мережі доступу: ця загроза включає компрометацію елементів мережі доступу (наприклад, базових станцій) для підробки даних конфігурації та запуску інших атак (наприклад, DoS)

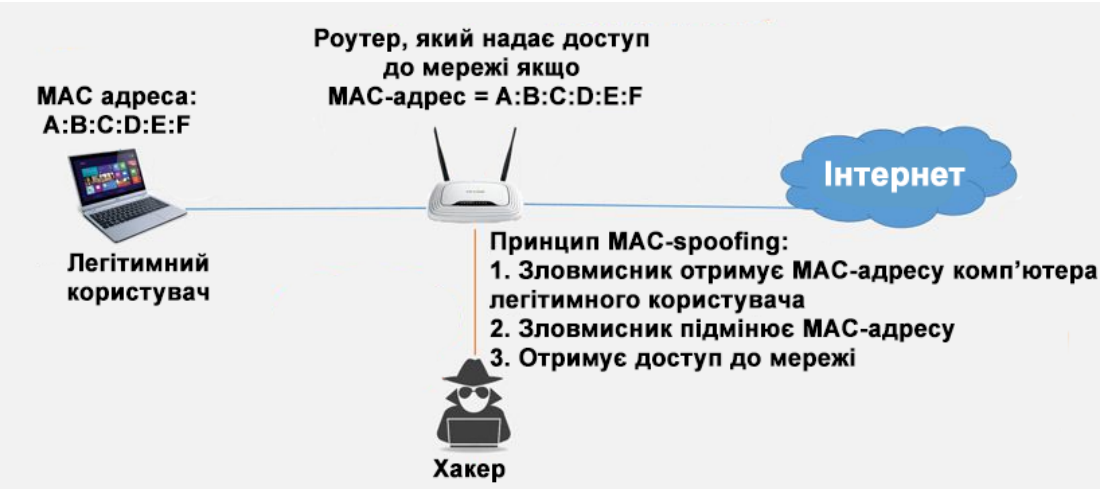

Рис. 2.5 Принцип дії MAC-spoofing

Радіозавади: загроза, в якій злочинець намагається зробити мережевий ресурс недоступним для його призначених користувачів заважаючи або порушуючи послугу мережі радіодоступу. Впровадження компрометованих пристроїв 5G у мережу радіодоступу представлятиме більш значну DoS загрозу.

Маніпуляція радіотрафіком: ця загроза розглядає маніпулювання мережевим трафіком на рівні базової станції. Атака "посередника" може бути розпочата на основі шахрайської базової станції, коли зловмисник маскує свою базову приймально-передавальну станцію (BTS) як реальну мережу BTS.

TCP Hijacking: загроза виникає коли зловмисник може переглядати пакети учасників мережі і посилати свої власні пакети в мережу. Атака використовує особливості встановлення з'єднання в протоколі TCP, і може здійснюватися як під час «потрійного рукостискання», так і під час з'єднання.

2.5 Загрози граничних обчислень мультисервісного доступу

Фальшивий або неправдивий шлюз MEC (Multi-Access Edge Computing, граничні/периферійні обчислення мультисервісного доступу): створюється сценарій, коли зловмисники можуть розгорнути власні шлюзи і пристрої. Ця загроза призводить до таких результатів, як і атака «посередника» (Man-in-the-middle attack)

Перевантаження граничного/периферійного вузла. Ця загроза стосується атак на граничні мережі, що руйнують околиці постраждалих мереж, на локальному рівні або сервісному рівні. Перевантаження може статися за допомогою флуду граничного вузла запитами або трафіком, спрямованим на цей компонент, ініційованим певними мобільними додатками або пристроями IoT.

Неправомірне використання відкритих граничних інтерфейсів прикладного програмування (API): зловживання відкритими API в вузлах граничних обчислень мультисервісного доступу здійснюється за рахунок

використання вразливостей у додатках MEC. Ця загроза може бути пов’язана з DoS, атакою «посередника», витоками конфіденційної інформації та маніпуляціями з VM.

2.6 Загрози віртуалізації

Неправомірне використання протоколу взаємозв'язку датацентрів (DCI, Data Centers Interconnect): віртуалізовані системи розгорнуті всередині датацентрів, отже, слід враховувати і загрози безпеки центрів обробки даних. Ця загроза стосується використання конкретних вразливих протоколів DCI (наприклад, відсутність аутентифікації та шифрування). Зловмисник може створити підроблений трафік таким чином, щоб він створював DoS-атаку на з'єднання DCI.

Неправомірне використання хмарних обчислювальних ресурсів: зловживання потужною обчислювальною інфраструктурою, включаючи як програмні, так і апаратні компоненти, може бути легко досягнуто за допомогою простого процесу реєстрації у провайдера хмарних обчислень. Користуючись перевагою над обчислювальною потужністю хмарних мереж, хакери можуть провести атаки за дуже короткий час. Наприклад, жорстокі атаки та DoS-атаки можуть бути запущені шляхом неправомірного використання потужності хмарних обчислень.

Обхід віртуалізації мережі: проблеми, пов’язані з поганою реалізацією та налаштуванням розділення мережі (network slicing) або неправильною ізоляцією даних, можуть призвести до втрати конфіденційності/приватності даних. Мережа, яка використовується різними орендарями, повинна гарантувати те, що в мережевий фрагмент потрапляє або залишає його лише легальний трафік, а також, що будь-який елемент комутації перевіряє та застосовує ізоляцію трафіку, встановлюючи законні правила потоку інформації. На рівні основної мережі ворожий суб'єкт використовує

вразливості гіпервізора та розкриває дані, що належать іншим орендарям мережі.

Зловживання віртуалізованим хостом: ця загроза стосується програм, що працюють на віртуалізованих хостах, відбувається неправомірне використання спільних ресурсів з віртуалізованого середовища. У віртуальних середовищах, де фізичні ресурси діляться між орендарями мереж, можуть відбутися неправомірні дії, що призводять до розкриття конфіденційної інформації. Хоч і прослуховування інформації є загальною загрозою у фізичних системах (наприклад, мережевих середовищах), її ефект посилюється ще більше у віртуальних середовищах.

2.7 Загрози фізичної інфраструктури

Маніпуляція апаратним обладнанням: ця загроза має на увазі включення прихованого апаратного чи програмного забезпечення до товару постачальником або вендором. Ця загроза може виникнути на початковій стадії впровадження продукту або під час технічного обслуговування із застосуванням неконтрольованих оновлень та нових функцій.

Природні катастрофи, що впливають на мережеву інфраструктуру: Ця катастрофа, класифікована як стихійна чи екологічна, стосується природних подій, таких як пожежі, повені та землетруси, які можуть вплинути на мережеве обладнання 5G, а отже, і на доступність сервісів на місцевому та регіональному рівні. Більше всього вразливі до стихійних лих обладнання для радіодоступу (наприклад, базові станції) та транспортна мережа.

Фізичний саботаж/вандалізм мережевої інфраструктури: ця загроза, класифікована як навмисна фізична атака, стосується дій, що вживаються суб'єктами, спрямованими на знищення, вимкнення або викрадення фізичних активів, що підтримують мережу 5G. Фізична атака критичних активів 5G може порушити, перешкодити і в кінцевому рахунку призвести до недоступності сервісів мережі. Незважаючи на існування механізмів фізичного захисту (наприклад, зовнішнє спостереження та камери

спостереження, замки безпеки, охоронці), все ще можуть відбуватися фізичні порушення та інсайдерські загрози.

Експлуатація формату UICC. Нові формати UICC можуть призвести до появи нових видів уразливих місць, які можуть бути використані для ексфільтрації даних, шахрайства або DoS атак. Різні типи нових компонентів UICC (наприклад, eUICC, iUICC, soft SIM тощо) вимагають нових протоколів управління. Ці протоколи можна використовувати для створення атак DoS щодо користувача або для сценаріїв шахрайства, включаючи видавання себе за інше лице.

Компрометація абонентського обладнання: нові формати абонентського обладнання, включаючи недорогі незахищені пристрої IoT, можуть ввести нові види вразливих місць, які можуть бути використані для атак на конфіденційність та цілісність даних користувачів. Зловживання на апаратному та програмному забезпеченні з боку абонентського обладнання для встановлення шкідливих компонентів можуть порушити конфіденційність та цілісність даних абонентів.

2.8 Загрози загального характеру

Відмова в обслуговуванні (DoS, Denial of Service): DoS - це загроза, коли злочинець намагається зробити мережевий ресурс недоступним для його призначених користувачів тимчасово чи на невизначений час заважаючи або порушуючи сервісам мережі. Атака включає генерацію величезної кількості запитів або трафіку таким чином, що мережа стає частково або повністю недоступною для постійних користувачів. Кілька видів загроз можуть призвести до відмови в службі. Атака, що поєднує декілька векторів атак, може призвести до розподіленої атаки DoS (DDoS, Distributed Denial of Service).

Витік даних, крадіжка та маніпулювання інформацією: це включає, але не обмежується ними, крадіжку особистої інформації через несанкціонований доступ до систем та/або мережі, несанкціонований доступ

та можлива публікація особистої інформації, конфіденційної інформації компанії або урядової чи державної інформації (засекречена інформація). Крадіжка, або витік інших типів даних, таких як облікові дані користувачів, ключі шифрування, журнали безпеки мережі, конфігурація програмного забезпечення тощо, можуть також допомогти зловмиснику в проведенні атак на мережі 5G.

Підслуховування: загроза, в якій злочинець намагається отримати несанкціонований доступ до програмних та комунікаційних рівнів з різних мережевих елементів 5G (контролер SDN, мережева функція, граничний вузол). Вона включає підслуховування даних абонента, конфіденційної інформації, системного часу, локації абонента, електронних повідомлень, сигналу даних, що передаються по мережі. Хакер здійснює моніторинг, шпигунство та/або підслуховування громадян країни та/або організацій для відстеження місцезнаходження та доступу до конфіденційної інформації.

Шкідливий код чи програмне забезпечення: загроза включає встановлення та розповсюдження шкідливого програмного забезпечення або впровадження певного коду чи програмного забезпечення всередину оновлень. Приклади шкідливого програмного забезпечення включають в себе зловмисне програмне забезпечення, віруси, трояни, SQL injections (впровадження SQL-коду), програмне забезпечення для несанкціонованого доступу, програмне забезпечення для спостереження. Приклад зловмисного програмного забезпечення в контексті 5G розглядає використання незареєстрованої VNF, яку можуть неправомірно встановити та зареєструвати в основній мережі з метою опублікування шкідливих API.

Атака на ланцюг поставок: це атака, яка прагне завдати шкоди організації, націлюючись на менш захищені елементи в мережі постачання. При цій атаці, вендор або постачальник послуг, навмисно вводить в продукт приховане шкідливе програмне забезпечення, обладнання і вразливі місця. Також, під цією атакою розуміється впровадження непідконтрольних оновлень програмного забезпечення, маніпуляція функціональними

можливостями, включення функції для обходу механізмів безпеки, бекдорів (backdoors), незадокументованих тестувальних функцій.

Ця загроза також пов'язана з діяльністю, здійсненою ненадійними сторонніми особами, що стосуються тестування, обслуговування, налаштування та експлуатації продукції. Сторонні особи отримують доступ до засобів управління мережею (як локально, так і через віддалений інтерфейс) для здійснення заходів з технічного обслуговування та надання технічної підтримки. Цей привілейований доступ до операцій, адміністрування та управління (OAM) мережі дає стороннім особам права для доступу до різних типів даних, таких як абонентська конфігурація системи та мережі, дані телеметрії.

Експлуатування недоліків у безпеці, управлінні та експлуатаційних процедурах. Ця загроза не пов'язана безпосередньо з 5G, вона стане актуальною, коли матиме справу зі складними технології та необхідністю впровадження операційних процедур для управління мережею.

Зловживання автентифікацією. Ця загроза може зачіпати кілька точок входу в мережу, таких як користувацьке обладнання (мобільні пристрої та IoT), інтерфейси операцій та управління, роумінг та вертикальні сервіси (vertical services). Ця загроза включає крадіжку облікових даних користувачів, використання методу «грубої сили» (brute-force, брутфорс) облікових записів користувачів, злам пароля та інші методи, які використовуються зловмисниками для неправомірного використання систем автентифікації мереж 5G.

Крадіжка особи (Identity theft) або підміна (spoofing): ця загроза може здійснитися, коли хакер визначає і використовує персональні дані людини, а потім маскується під нею до наступних атак. Підробка особистості - це загроза, яка може вплинути на будь-який компонент програмного забезпечення або людину. У цій атаці зловмисник підробляє особу законного власника та взаємодіє з мережевими функціями, контрольованими легітимним власником, щоб викликати кілька інших типів атак. Для підміни

чи крадіжки даних користувачів мережі 5G також можуть використовуватися брутфорс користувацьких акаунтів та злам паролів.

2.9 Аналіз загроз в непублічній мережі

Non-Public Network, NPN – непублічна 5G мережа, яка під'єднана до зовнішнього світу через канали загального користування. Такі мережі будуть в якості типових в найближчому майбутньому у всіх країнах. Потенційне середовище для розгортки мереж з такою конфігурацією - «розумні» міста, «розумні» компанії, офіси великих підприємств, а також інші аналогічні локації, які мають високий рівень контрольованості.

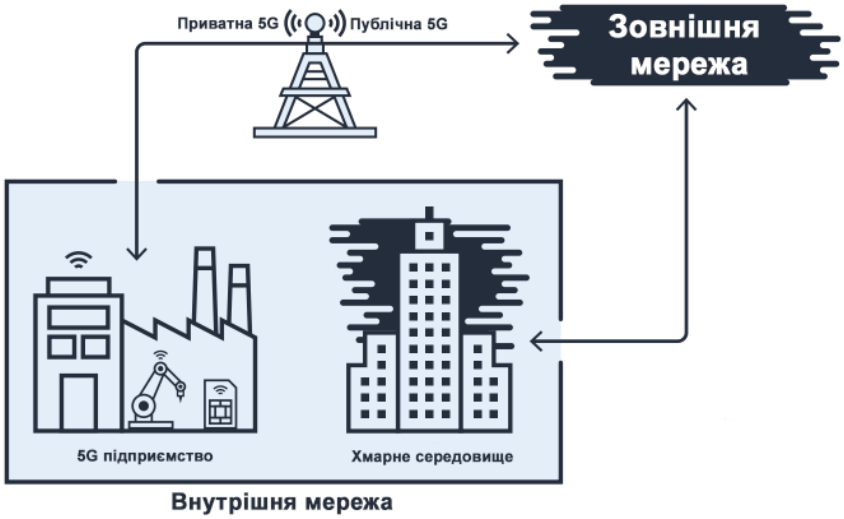

Рис. 2.6 Непублічна 5G мережа [13] [14]

З рис. 2.6. видно, що NPN має фундаментальну вразливість у своїй конструкції. Працююча у внутрішніх мережах система безпеки NPN, захищає об'єкт і його приватне хмарне сховище, системи безпеки зовнішніх мереж - свою внутрішню інфраструктуру. Трафік між зовнішніми мережами і NPN вважається безпечним, оскільки виходить з захищених систем, проте по факту його нічого не захищає. На цьому відрізку ділянки видимий IT-моніторинг безпеки - відсутній. Багато видів атак, можуть скомпрометувати інформацію, а отже, і саму 5G мережу.

В результаті цього, виникають декілька можливих сценаріїв атак на 5G мережі, які експлуатують:

- Вразливості SIM-карт

- Вразливості мережі
- Вразливості систем ідентифікації

2.9.1 Вразливості SIM-карт

SIM-карта представляє з себе складний пристрій, на якому є навіть цілий набір вбудованих додатків - SIM Toolkit, STK. Як приклад, одна з таких програм - S@T Browser – в теорії, може використовуватися для перегляду внутрішніх сайтів оператора, проте на практиці вона вже давно забута і не отримувала оновлень з 2009 року, оскільки зараз ці функції виконують інші програми.

Проблема в тому, що S@T Browser виявився вразливим: спеціально підготовлена службова SMS зламує SIM-карту і змушує її виконувати необхідні для зловмисника команди, причому користувач пристрою або телефону не помітить нічого незвичайного. Ця атака отримала назву Simjaker або Simjacking. Вона дає масу можливостей для зловмисників. Принцип її роботи зображено на рис 2.7.

Зокрема, ця атака дозволяє передати зловмисникові дані про місцезнаходження абонента, ідентифікатор його пристрою (IMEI) і базової станції (Cell ID), а також змусити телефон набрати якийсь номер, відправити SMS, відкрити посилання в браузері і навіть відключити SIM-карту.

В 5G мережах ця вразливість SIM-карт стає серйозною проблемою, беручи до уваги кількість підключених пристроїв в мережі. Не дивлячись на те, що організація SIMAlliance розробила нові стандарти SIM-карт для 5G з підвищеною безпекою, в мережах п'ятого покоління можливе використання SIM-карт старого типу як і раніше.

Використання Simjacking дозволяє примусово переключити SIM-карту в режим роумінгу і змусити її підключитися до базової станції, яку контролює зловмисник. При цьому зловмисник отримує можливість змінювати налаштування SIM-карти, що дає змогу прослуховувати телефонні розмови, впроваджувати шкідливе ПО і проводити різні види атак з

використанням пристрою, що містить зламану SIM-карту. Цьому сприяє факт, що взаємодія з пристроями в роумінгу відбувається в обхід процедур безпеки, прийнятих для пристроїв в «домашній» мережі.

Рис. 2.7 Атака Simjacking в 5G мережі [13] [14]

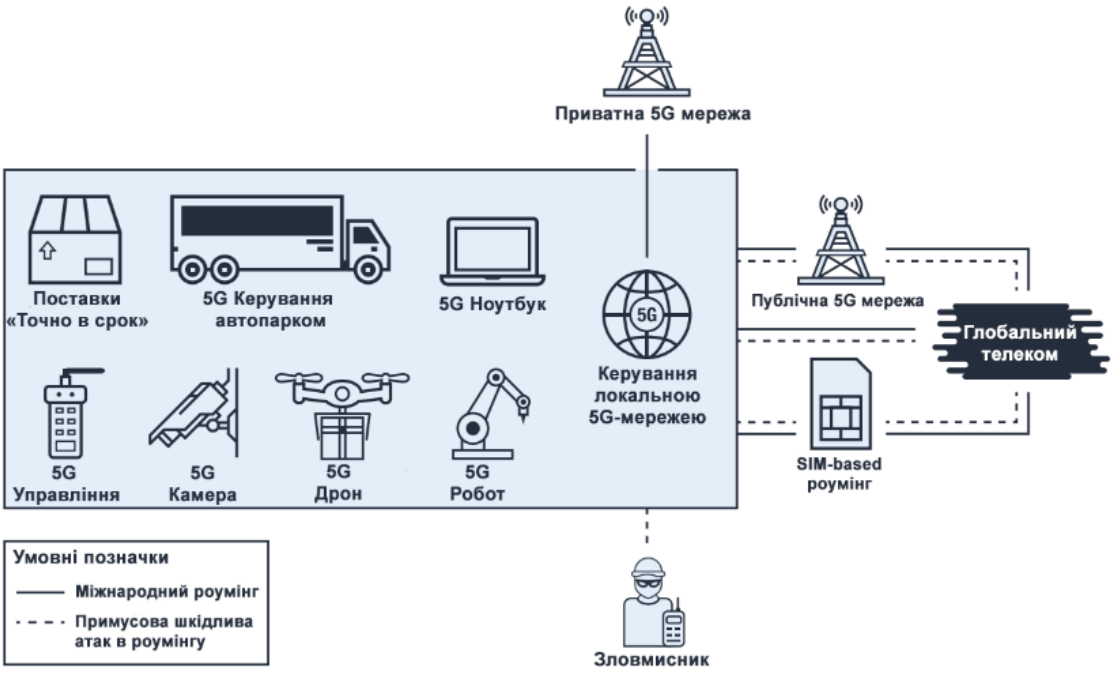

Рис. 2.8 Зловмисне шкідливе використання роумінгу [13] [14]

2.9.2 Вразливості мережі

Хакери можуть змінювати налаштування скомпрометованої SIM-карти для вирішення своїх завдань. Відносна легкість і скритність атаки Simjaking дозволяють проводити її на постійній основі, захоплюючи контроль над все

новими і новими пристроями, використовуючи такі атаки як low and slow attack і salami attack. Назви атак говорять самі за себе – мережа повільно та терпеливо «нарізається» на шматочки, подібно до скибочок салямі. Відстежити вплив таких атак на мережу вкрай складно, а в умовах складної розподіленої мережі 5G - практично нереально.

А оскільки мережі 5G не мають вбудованих механізмів для контролю безпек SIM-карт, зловмисники поступово будуть отримувати можливість встановити всередині комунікаційного домена 5G свої правила, використовуючи захоплені SIM-карти для крадіжки коштів, авторизації на мережевому рівні, встановлення шкідливого програмного забезпечення та іншій незаконній діяльності.

Особливу тривогу викликає поява на хакерських форумах інструментарію, що автоматизує захоплення SIM-карт за допомогою Simjaking, оскільки застосування таких засобів для мереж п'ятого покоління дає зловмисникам практично необмежені можливості з масштабування атак і модифікації довіреного трафіку.

2.9.3 Вразливості ідентифікації

SIM-карта використовується для того, щоб ідентифікувати пристрій в мережі. Якщо SIM-карта активна і має позитивний баланс, пристрій автоматично вважається легітимним і не викликає ніяких підозр на рівні систем виявлення проблем з безпекою. Між тим, вразливість самої SIM-карти робить уразливою всю систему ідентифікації. IT-системи безпеки просто не зможуть відстежити пристрій, який був незаконно підключений, якщо він зареєструється в мережі за допомогою викрадених ідентифікаційних даних через Simjaking.

З цього виходить, що зловмисник, який підключився до мережі через зламану SIM-карту отримує доступ до мережі на рівні справжнього власника, оскільки IT-системи вже не перевіряють пристрої, які пройшли ідентифікацію на мережевому рівні.

Гарантована ідентифікація між програмним і мережевим рівнем додає ще одну проблему: злочинці можуть навмисне створювати «шум» для систем виявлення вторгнень в мережу, постійно виконуючи різні підозрілі дії від імені захоплених ними пристроїв. Оскільки робота автоматичних систем виявлення проблем з безпекою базується на аналізі статистики, порогові значення для сигналу тривоги будуть поступово збільшуватися, забезпечивши відсутність реакції на реальні атаки. Такі тривалі дії цілком в змозі змінити функціонування всієї мережі і створити «сліпі зони» для систем виявлення. Зловмисники, які контролюють такі зони, можуть проводити атаки на дані всередині мережі та на фізичні пристрої, організувати відмову в обслуговуванні або наносити іншу шкоду.

Висновки до розділу: в даному розділі проаналізовано основні вразливості, загрози, слабкі місця та можливі атаки на 5G мережі. В мережах 5G не тільки залишилися вразливості, які були в минулих поколіннях, але і з’явилися нові загрози безпеки. Більш того, деякі вже давно відомі види атак несуть з собою більшу небезпеку, оскільки питання та проблеми безпеки 5G стосуються не лише смартфонів та смарт-годинників, як це було в 4G мережах, а і таких серйозних речей та пристроїв як автомобілі з автопілотом, розумні літаки, розумні міста, в яких неправомірне використання недоліків та вразливостей мережі зловмисниками може привезти до катастрофічних наслідків.

РОЗДІЛ 3.

ЗАБЕЗПЕЧЕННЯ ЗАДАНИХ ПОКАЗНИКІВ БЕЗПЕКИ

З більш широким спектром застосувань сервісів 5G та його критичній ролі в обслуговуванні суспільства для соціального, економічного зростання та громадської безпеки, вектор загроз для 5G також збільшується. Мотивація атакувати 5G мережі тепер буде вищою, ніж у попередніх мережевих поколіннях. Все більше шансів на те, що 5G стане ключовою ціллю для злочинних дій, керованих різними мотивами, такими як державні політичні мотиви, суперництво, конкуренція, картелі організованої злочинності, шпигунство та кібервійни.

Зловмисники продовжують оновлювати та знаходити нові способи ухилення від виявлення атак, навчившись використовувати соціальну та фінансову систему для своїх потреб. З розвитком цифрових платіжних систем та таких технологій, як Біткойн, злочинцям буде набагато простіше залишатися непоміченими та продовжувати отримувати фінансові вигоди.

Вектор загроз 5G буде безмежним і буде сильно залежати від обладнання кінцевих користувачів, таких як мобільні телефони, промислові товари, датчики, домашня автоматизація, автоматизовані машини, корпоративні мобільні мереж. З таким більшим спектром загроз, як вже розглядалось в попередньому розділі, буде охоплено пристрої кінцевих користувачів від RAN (мереж радіодоступу) до мобільних базових мереж. Кожна окрема область мережі 5G опиниться під загрозою. Це буде серйозним викликом безпеки, для рішення проблеми необхідно буде активізувати та будувати надійну систему захисту, яка може захищати мережі 5G від початку до кінця.

3.1 Вдосконалена модель безпеки 5G

Для захисту 5G від вдосконалених і складних видів загроз потрібна розвинена модель безпеки (як показано на рис 3.1), яка пропонує глибокий

захист не тільки від існуючих, але і від еволюціонуючих та нових видів загроз, а також загроз нульового дня. Це вимагатиме чітко визначеної стратегії безпеки та плану захисту різних компонентів для мережі 5G, включаючи кінцеві пристрої та кінцевих користувачів. Ефективна стратегія безпеки може бути розроблена на основі телеметричних даних, отриманих за допомогою добре розробленої системи спостереження. Необхідно визначити процеси та інструменти для участі у виявленні атак та нападів на систему, блокувати їх та розвивати систему захисту мережі.

Рис 3.1 Посилена модель безпеки 5G розпізнавання загроз [22]

Забезпечення належного рівня безпеки є обов'язковим для постійно змінюючихся видів загроз та атак на системи безпеки 5G мереж. Для посилення безпеки та захисту даних користувачів, модель безпеки має відповідати наступним вимогам та параметрам:

1) *Конфіденційність*: в моделі безпеки 5G конфіденційність даних є однією з основних вимог безпеки; властивість, яка може захистити передачу даних від розголошення її стороннім особам та від пасивних атак (тобто, прослуховування та підслуховування). Враховуючи архітектури 4G-LTE та 5G, будь-які дані користувача повинні бути конфіденційними та захищеними

від несанкціонованих користувачів. Стандартні алгоритми шифрування даних широко прийняті для реалізації конфіденційності даних у мережевих додатках 5G (наприклад, мережах транспортних засобів, моніторингу стану здоров'я тощо). Симетричні криптосистеми можуть бути використані для шифрування та дешифрування даних 5G одним і тим же приватним криптографічним ключем. Вони обмінюються між комунікаційними об'єктами (наприклад, відправником та одержувачем).

2) *Цілісність*: запобігання втручанню та втраті інформації під час її переміщення з однієї точки в іншу. Цілісність даних в 5G NR захищена аналогічно 4G. У 5G NR цілісність захищена бездротовим трафіком даних на рівні протоколу конвергенції пакетних даних (PDCP). У 4G LTE захищеність цілісності забезпечується лише для шару (рівня) без доступу (NAS) та шару доступу (AS). Однак однією з головних відмін у захисті цілісності 5G є те, що 5G NR також забезпечує захист цілісності площини користувача. Це важливо, оскільки в 4G такої функції не було. Ця нова функція корисна для невеликих передач даних, особливо для обмежених пристроїв IoT. Більше того, механізм аутентифікації 5G 5G-AKA використовує захищену телесигналізацію. Це гарантує, що жодна сторона, яка не має права, не може змінювати та отримувати доступ до інформації, яка передається в ефірі.

3) *Доступність*: у області 5G доступність мереж - це забезпечення доступності мережевих ресурсів тоді, коли вони будуть потрібні законним користувачам, оскільки доступність впливає на репутацію постачальника послуг. Іншими словами, доступність забезпечує високу ймовірність ефективності мережевої інфраструктури. Вона також вимірює стійкість мережі проти активних атак, наприклад, DoS-атак. Атака DoS може погіршити продуктивність мережі. Однак за допомогою надширокосмугового мобільного зв’язку (eMBB) та надвисокого надійного MachineType-зв'язку (uMTC) доступність мережі може бути досягнута як мінімум на 95% та 99,99% відповідно, при їх застосуванні в 5G мережі.

4) *Централізована політика безпеки*: архітектури безпеки 3GPP 4G не можуть безпосередньо застосовуватися для використання в мережах 5G, оскільки вони присвячені традиційній моделі довіри оператор-абонент. Тому для підтримки нових інновацій (таких як NFV та SDN) існує потреба у централізованій системі управління політикою безпеки, яка забезпечує зручність доступу користувачів до додатків та ресурсів. Для цього можна використовувати структуру управління безпекою на основі політик для підтримки централізованого управління безпекою для 5G. Цей метод полягає в тому, що він використовується для прийняття рішень з проблемами безпеки на основі політик, встановленими адміністратором мережі, або оператором. Крім того, оператори можуть включити Security-as-a-Service (SaaS) як потенційне рішення проблем з безпекою для ряду клієнтів, наприклад таких як вендори IoT.

5) *Видимість*: дозволяє ефективно вирішити основні проблеми мережі для забезпечення безпечного середовища. Мережам 5G необхідно використовувати комплексні стратегії наскрізного (end-to-end) захисту які повинні охоплювати всі рівні мережі. Для реалізації такого всебічного механізму безпеки 5G-оператори повинні мати повну видимість, перевірку та контроль над усіма рівнями мережі. Технології 5G повинні бути інтегровані з відкритими API для управління політикою безпеки. Таким чином, мережа 5G може мати послідовну політику безпеки як програмного, так і апаратного забезпечення в мережі. Покращена видимість всієї мережі та політик безпеки допоможуть реалізувати нові посилені механізми безпеки, що підходить для нових послуг 5G. Більше того, покращення видимості дозволяє запобігти загрозам, що керують даними, знаходити та ізолювати заражені пристрої до того, як вони вчинили атаку на мережу.

3.2 Моніторинг безпеки

З еволюцією мобільних мереж від LTE до LTE Advanced і відтепер до технології 5G, мобільні RAN та базові мережі також розвиваються і

витісняються новими технологіями, такими як Cloud RAN, NFV та SDN. Для мобільних операторів надзвичайно важливо мати реальну видимість та вести спостереження за своїми мережами у режимі реального часу, і не лише забезпечувати кращу надійність обслуговування, але й захищати їх критичні мережеві інфраструктури від загроз безпеці. Успадковані рішення мереж минулих поколінь для моніторингу безпеки мобільних пристроїв не були розроблені для захисту мереж на базі SDN або NFV і не мали або обмежували можливості інтегруватися з сучасними технологічними компонентами мобільної мережі, і тому їх потрібно замінити рішеннями з моніторингу безпеки, які пропонують більш високу продуктивність, масштабованість та можливість інтегрувати та працювати з цими новими мобільними технологіями. Рішення з моніторингу безпеки для мереж 5G повинні надавати можливість контролювати та перевіряти як сигнальний трафік, так і трафік даних у кількох точках мережі, починаючи від UE до RAN і аж до компонентів базової мережі 5G. Рішення повинно бути в змозі не тільки перевіряти IPv4 та IPv6, але й пропонувати видимість для інших протоколів, таких як TCP, UDP, GRE тощо. Замість традиційної інспекції на основі пакетів 5G мережі можуть також використовувати контроль SDN та розділення площини даних та здійснювати централізований моніторинг трафіку потоку мережі для більш глибокої видимості та кореляції руху трафіку всередині мережі. Моніторинг безпеки мобільної мережі повинен пропонувати деякі попередні служби безпеки, такі як:

- тести на вразливість;
- регулярні перевірки стану безпеки для всієї мережі;
- видимість потоку даних в мережі;
- система управління сповіщеннями про безпеку;
- моніторинг та перевірка трафіку.

3.3 Безпека фізичної інфраструктури 5G мереж

Зв’язок набуває все більшого значення в сучасному суспільстві, оскільки комунікація в соціальних, економічних та промислових системах стає все більш цифровою, бездротовою та взаємозалежною, споживчий ринок глобально розширюється, а також збільшується попит і пропозиція. Стоячи на межі технологічної революції 5G, через її масштаби, обсяг та складність її вплив на суспільство передбачаються неабиякі можливості та переваги, а також великі загрози.

Комунікаційні структури - це критично важлива інфраструктура. Однією з найактуальніших проблем сьогодні є виділення обмежених ресурсів для зменшення таких можливих ризиків, як природні та / або техногенні небезпеки, які є ключовими для фізичних інфраструктур. Якщо цього не зробити, це, безумовно, матиме величезні наслідки, оскільки величина ризику є колосальною. Не через економічну цінність самої фізичної інфраструктури, а тому, що добробут і сталий розвиток суспільства сьогодні і в майбутньому сильно залежать від можливостей цієї системи продовжувати прогресувати і надавати надійні послуги та пристосовуватися до еволюції та розвитку цивілізації.

Управління ключовими фізичними інфраструктурами мереж зв'язку може бути досягнуто шляхом адаптації існуючих або розробки нових стандартів та методологій проектування.

Для розробки методичних рекомендацій щодо досягнення більш ефективних стандартів та методологій проектування неодмінно необхідно визначити найважливіші змінні, що контролюють структурну крихкість та стійкість системи. Необхідність захисту критичної інфраструктури повинна бути збалансована із обсягом наявних ресурсів, наприклад технічних та фінансових.

Для того, щоб можна було готувати рішення проблем з безпекою, спочатку необхідно закріпити контекст проблеми. Тому відповідні технічні,

соціальні, економічні та регуляторні особливості комунікаційних систем минулого, сьогодення та передбачуваного майбутнього потребують належного обговорення. Наприклад, характеристика основних фізичних інфраструктур, топологія існуючих мереж та точне визначення основних проблем, які слід вирішити для досягнення намічених цілей, є частиною цього процесу.

Далі слід застосувати методи оцінок ризику. Це завдання охоплює визначення ризиків, їх аналіз та оцінка. Воно полягає у формальному, систематичному та всебічному складанні, огляді та використанні доступної інформації щодо відповідних сценаріїв небезпеки. Згодом слід встановити зв’язки між небезпеками, наслідками та причинами їх виникнення. У зв'язку з цим потрібні дослідження щодо небезпек, щодо яких наявні дані є неповними, недостатніми або навіть відсутні.

Оцінка ризику - це процес вивчення та судження про значення ризиків. По-перше, слід встановити критерії прийняття ризику, а також визначити прийнятний та неприйнятний рівень ризику, наприклад, дотримуючись принципу ALARP (мінімальний практично прийнятий ризик). Крім того, може бути розроблений перелік із цілим рядом альтернативних заходів (активних чи пасивних, профілактичних чи захисних) для управління ризиками, які перевищують прийнятний рівень ризику.

Останній крок управління ризиками - це контроль ризиків. Він включає визначення заходів, найбільш підходящих для управління ризиками, визначення ефективності цих заходів. Для кожного з обраних заходів щодо урегулювання ризиків слід оцінити залишкові ризики та оптимізувати розподіл ресурсів.

3.4 Потенційні рішення проблем з безпекою

Нові технології, такі як SDN та NFV, можуть вирішити проблеми з безпекою більш економічно. У SDN контролер може збирати статистику мережі через інтерфейс південний інтерфейс API (Southbound interface), щоб

побачити, чи зростає рівень трафіку, а отже і виявити можливий шкідливий трафік. Безпека роумінгу і загальномережеві обов'язкові політики безпеки можуть бути досягнуті за допомогою централізованих систем, які мають глобальну видимість дій користувачів і поведінки мережевого трафіку, наприклад SDN. “Шторми” 5G-сигналу (5G signaling storms) будуть більш складними через надмірне підключення UE, невеликих базових станцій і високої мобільності користувачів. C-RAN і граничні обчислення є потенційними вирішувачами проблем для цих завдань, але при розробці цих технологій необхідно враховувати збільшення сигнального трафіку як важливий аспект майбутніх мереж.

3.4.1 Рішення проблем безпеки в мобільних хмарах

Більшість запропонованих заходів безпеки в MCC (Mobile Cloud Computing / (Мобільні хмарні обчислення) обертаються навколо стратегічного використання технологій віртуалізації, редизайну методів шифрування і динамічного розподілу точок обробки даних. Таким чином, віртуалізація є природним варіантом захисту хмарних служб, оскільки кожен кінцевий вузол підключається до певного віртуального екземпляру об’єкта в хмарі через віртуальну машину (VM). Це забезпечує безпеку за рахунок ізоляції віртуального з'єднання кожного користувача від інших користувачів. Аналогічним чином, сервісно-базовані обмеження також дозволять забезпечити безпечне використання технологій хмарних обчислень. Наприклад, можна використовувати інфраструктуру «безпечний обмін і пошук відео в реальному часі в мобільній хмарі» (Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud), яка використовує хмарну платформу і технологію 5G для захисту хмарних сервісів і дозволяє мобільним користувачам обмінюватися відео в реальному часі в хмарному середовищі з підтримкою 5G. На відміну від існуючих рішень, де користувачі з загальними посиланнями можуть отримати доступ до онлайн-відеопотоків, ця архітектура обмежує і надає доступ тільки авторизованим глядачам.

Для забезпечення безпеки мобільних терміналів використання антивірусних програм цілком може підвищити загальну стійкість до атак шкідливих програм. Антивірусні додатки встановлюються на мобільному терміналі або розміщуються і обслуговуються безпосередньо з хмари.

Для забезпечення безпеки мереж радіодоступу (RAN) пропонується хмарна платформа, тобто C-RAN для оптимізації і забезпечення більш безпечних мереж радіодоступу для хмарних середовищ в 5G. C-RAN може динамічно підвищувати наскрізну (end-to-end) продуктивність служб MCC в бездротових мережах наступних поколінь. Однак для того, щоб C-RAN задовольнив цей попит, він повинен забезпечити високий рівень надійності, який можна порівняти з традиційними оптичними мережами, такими як синхронна цифрова ієрархія (SDH), і один із способів досягнення цього - масове впровадження таких механізмів, як захист волоконно-кільцевої мережі, які в даний час в основному використовуються в промисловості та енергетиці.

3.4.2 Рішення проблем безпеки в SDN та NFV

Завдяки логічно централізованій площині управління з глобальним мережевим представленням і програмованістю SDN полегшує швидку ідентифікацію загроз за допомогою циклу збору інформації та даних з мережевих ресурсів, станів і потоків. Таким чином, архітектура SDN підтримує активний моніторинг безпеки, аналіз трафіку і системи реагування для полегшення мережевої експертизи, зміни політик безпеки і впровадження служб безпеки. Послідовні політики мережевої безпеки можуть бути розгорнуті по всій мережі завдяки глобальній видимості мережі, в той час як системи безпеки, такі як брандмауери і системи виявлення вторгнень (IDS), можуть використовуватися для конкретного трафіку шляхом оновлення таблиць потоків комутаторів SDN.

Забезпечити безпеку в NFV можна використовуючи довірене завантаження (Trusted computing), віддалену верифікацію та перевірку

цілісності віртуальних систем і гіпервізорів. Ці рішення служать для забезпечення апаратного захисту приватної інформації та виявлення пошкодженого програмного забезпечення у віртуалізованих середовищах.

3.4.3 Рішення проблем безпеки в каналах зв’язку

5G потребує належної безпеки каналів зв'язку не тільки для запобігання виявлених загроз безпеки, але і для підтримки додаткових переваг SDN, таких як централізоване управління політикою, програмованість і видимість стану глобальної мережі. IPsec є найбільш часто використовуваним протоколом безпеки для захисту каналів зв'язку в сучасних телекомунікаційних мережах, таких як 4G-LTE. Для захисту каналів зв'язку 5G можна використовувати тунелювання IPsec. Крім того, безпека зв’язку LTE забезпечується за рахунок інтеграції різних алгоритмів безпеки, таких як аутентифікація, цілісність і шифрування. Однак основними проблемами в таких існуючих схемах забезпечення безпеки є високе споживання ресурсів, високі накладні витрати і відсутність координації. Таким чином, ці рішення не є життєздатними для критичної інфраструктури зв'язку в 5G. Більш високий рівень безпеки критичного зв'язку досягається за рахунок використання нових механізмів безпеки, таких як безпека фізичного рівня, прийняття радіочастотної (RF) дактилоскопії, використання асиметричних схем безпеки і динамічна зміна параметрів безпеки в залежності від ситуації. Аналогічно, зв'язок між кінцевими користувачами може бути захищений за допомогою криптографічних протоколів, таких як протокол ідентифікації хоста HIP (Host Identity Protocol).

3.4.4 Рішення проблем конфіденційності в 5G

Мережа 5G повинна втілювати в собі підходи privacy-by-design, коли конфіденційність розглядається з самого початку в системі і багато необхідних функцій повинні бути доступні вбудованим чином. Підхід гібридної хмари необхідний там, де мобільні оператори можуть зберігати і

обробляти високочутливі дані локально і менш чутливі дані в загальнодоступних хмарних сховищах. Таким чином, оператори матимуть більше доступу і контролю над даними і зможуть вирішувати, де їх використовувати. Аналогічним чином, сервісно-орієнтована конфіденційність в 5G призведе до більш життєздатного рішення для збереження конфіденційності.

5G потребуватиме кращих механізмів мінімізації даних, прозорості, відкритості та контролю доступу. Отже, під час стандартизації 5G слід враховувати чіткі норми та законодавство про конфіденційність. Регулюючий підхід можна класифікувати на три типи. По-перше, це регулювання на рівні уряду, де уряди в основному приймають норми щодо конфіденційності для конкретних країн та через багатонаціональні організації, такі як ООН (ООН) та Європейський Союз (ЄС). По-друге, це галузевий рівень, де різні галузі та групи, такі як 3GPP, ETSI та ONF спільно розробляють найкращі принципи та практики для захисту конфіденційності. По-третє, регулювання на рівні споживачів, де бажана конфіденційність забезпечується шляхом врахування вимог споживачів. Для конфіденційності місцеположення слід застосовувати методи, засновані на анонімності, де реальну особу абонента можна було б приховати та замінити псевдонімами. Практики, засновані на шифруванні, також корисні в цьому випадку, наприклад, повідомлення можна зашифрувати перед відправкою до постачальника послуг Location-based service (LBS). Такі методи, як обфускація або заплутання коду, також корисні, коли якість інформації про місцезнаходження знижується з метою захисту конфіденційності місцеположення. Більше того, алгоритми, засновані на маскуванні місцеположення, є досить корисними для обробки деяких основних атак на конфіденційність місцеположення, таких як часові та граничні атаки.

3.4.5 Рішення проблем безпеки граничних обчислень

На рис. 3.2 показана необхідність у захисті кінцевих точок (захист від шкідливих програм, захист від 0day і 1day на кінцевих точках). Це не тільки захищає UE (наприклад, телефон, iPad), але і RAN, не дозволяючи створювати ботнет для атаки на RAN. Оператори матимуть свої власні варіанти використання, які будуються на цьому фундаменті.

Основоположною для всієї безпеки є "видимість". Видимість забезпечує постійно оновлювану картину того, як поводить себе мережа. Інформація про загрози робить цю систему оперативною щодо відомих і невідомих загроз.

Рис 3.2 Безпека в MEC

Спочатку потрібно переконатися що є в мережі ненормальним або аномальним, а потім необхідно сегментувати мережу, щоб уникнути поширення загроз і компрометації інших функцій або робочих навантажень. В сірому блоці на рис. 3.2 різні елементи керування, що використовуються в цьому місці мережі, застосовуються для послаблення загроз DDoS (об'ємних і прикладних), загроз веб-додатків через файрвол веб-додатків (WAF, Web application firewall), захисту API і захисту від шкідливих програм. Ці елементи управління забезпечують захист граничних (перефирійних) обчислень.

3.4.6 Виявлення загроз

Належна видимість системи, сегментація, безпека на рівні DNS і виявлення аномальних потоків даних - все це забезпечує базовий рівень безпеки для віртуалізованої частини архітектури 5G. На рис. 3.3 показано, як належна видимість (аналіз потоків, облік потоків і трафіку, інформація про загрози, оновлювана в режимі реального часу) і аналіз поведінки системи дозволяють оператору виявляти загрози, що впливають на ядро мережі 5G.

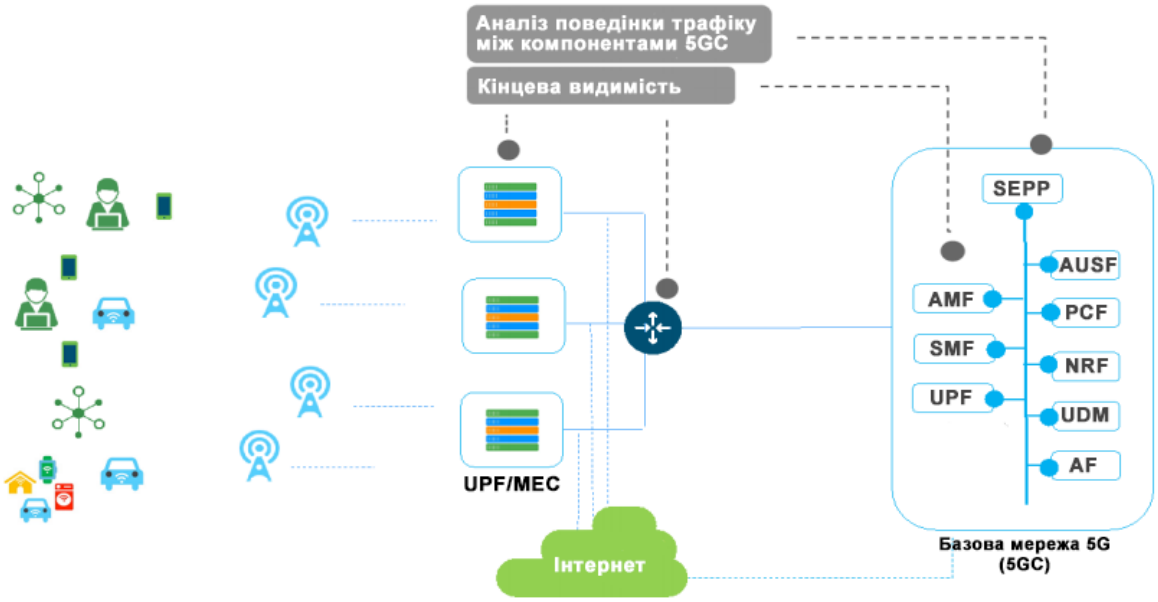

Рис. 3.3 Виявлення загроз в 5G мережі

3.4.7 Безпека Інтернету речей

Існує кілька способів зменшити та пом'якшити загрози IoT за допомогою технології 5G.

Безпека пристроїв IoT: конфіденційні дані в незахищених місцях фізичних пристроїв повинні бути зашифровані і захищено їх цілісність. Пристрої повинні криптографічно перевіряти прошивку і програмні пакети при завантаженні або оновленні, а також підтримувати можливість отримання віддалених оновлень прошивки навіть у разі зараження шкідливими програмами. Необхідно забезпечити достатній обсяг пам'яті для автоматичного відкату в разі збою оновлення. Також шкідливий відкат на старіші версії програмного забезпечення / мікропрограмного забезпечення,

які знову вводять старі вразливості, повинен бути запобіжений. Необхідність в ізоляції безпеки між додатками пристроїв має вирішальне значення. Один з варіантів забезпечити апаратну ізоляцію між додатками - використовувати підхід "корінь довіри" (RoT), щоб запобігти компрометації ОС, що зображений на рис. 3.4 Хоча ця функціональність зазвичай забезпечується спеціалізованим апаратним обладнанням, вона також може бути реалізована за допомогою довірених середовищ виконання (TEE, Trusted Execution Environments). TEE ізольований від середовища виконання на стороні клієнта в якій знаходиться ОС і додатки мобільних пристроїв, яке називається Rich Execution Environment (REE), або «функціонально багата середа виконання» в звичайних процесорах. Для недорогих пристроїв переважно використовувати TEE. Набір специфікацій TEE знаходиться у відкритому доступі в GlobalPlatform.

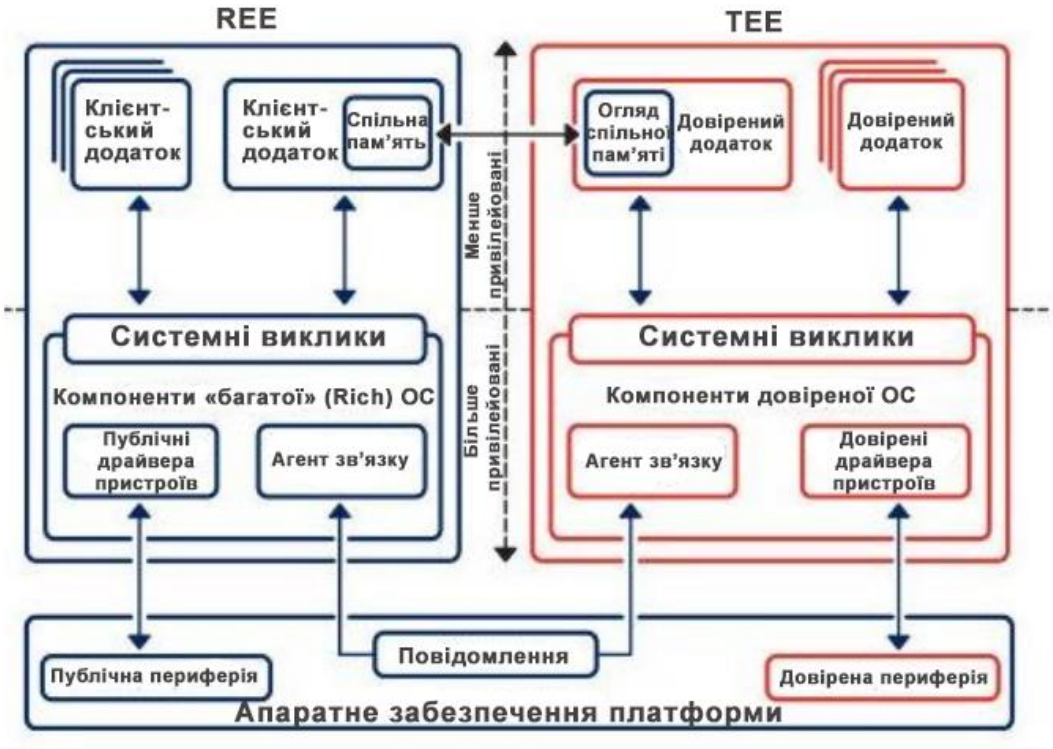

Рис. 3.4 Підхід Root-of-Trust («корінь довіри») [16]

Сучасні криптографічні алгоритми, навіть асиметричні, значно швидше застарілих алгоритмів і краще підходять для Інтернету речей. Легку криптографію (Lightweight cryptography) можна бути примінити для деяких сценаріїв.

Безпека мережі: мобільні оператори можуть використовувати своє унікальне положення в просторі Інтернету речей як постачальники послуг зв'язку і платформ. Такі технології, як LTE-M і NB-IoT, є чудовими рішеннями, призначеними для забезпечення глобального зв'язку, пропонуючи набагато більш високу надійність в порівнянні з неліцензійним доступом. Мобільні мережі можуть підвищити безпеку Інтернету речей, забезпечуючи управління пристроями і безпечне завантаження, а також перевіряти надійність розташування пристроїв або платформ. Як правило, облікові дані пристрою попередньо ініціалізуються на знімних UICC. Вбудований UICC (eUICC) забезпечує віддалену ініціалізацію і управління обліковими даними. Фактично генеруючи облікові дані на пристрої, можна знизити ризик порушення безпеки. Логічним наступним кроком є використання TEE, який вже інтегрований в процесор основної смуги частот (BBP). Ця комбінація пропонує такі переваги, як зниження апаратних витрат і енергоспоживання, підвищення швидкості, а також гнучкість безпечної модифікації облікових даних.

Безпека додатків: додатки Інтернету речей слід розміщувати на захищених платформах, використовуючи коріння довіри в хмарній інфраструктурі. Обмін даними між додатками IoT або між додатками і пристроями може бути забезпечений за допомогою полегшених протоколів безпеки IETF, таких як платформа авторизації на основі OAuth (IETF), що підходить для обмежених середовищ. Для захисту від посередників одного лише використання IPsec і TLS може виявитися недостатньо. Ці протоколи підтримують лише моделі довіри, які можуть гарантувати повністю довірені кінцеві точки. Дозвіл на доступ до інформації має надаватися тільки тому кому це необхідно знати. Для досягнення цієї мети наскрізна безпека повинна бути забезпечена на рівні додатків. Використання інформаційних контейнерів на рівні додатків, які здатні забезпечити конфіденційність, цілісність і аутентифікацію джерела, є кращим рішенням для захисту обміну повідомленнями.

3.4.8 Безпека MIoT

Щоб запобігти порушенню роботи сервісів 5G, викликане ботнетами MIoT, використовуваними для DDoS-атак на RAN, і забезпечити відмовостійкість сервісу 5G, необхідні обдумані вимоги безпеки для мережі 5G. Основою цих вимог безпеки є виявлення і протистояння DDoS-атакам проти 5G RAN, які також можуть бути класифіковані як функції перевантаження 5G RAN. Реалізація цих вимог безпеки включатиме співпрацю між спільнотою стандартів 5G, операторами 5G та постачальниками 5G RAN. Хоча унікальна реалізація мережі 5G кожного оператора може забезпечити деякий обмежений захист від цього типу атак, це буде тільки половинчаста міра, оскільки компоненти 5G RAN повинні будуть відігравати важливу роль у справжньому та ефективному виявленні та протистоянню цим типам атак у реальному часі. Саме тут спільнота стандартів 5G і вендори 5G RAN будуть відігравати ключову роль.

Щоб виявити DDoS-атаку на 5G RAN оператора, викликану ботнетами MIoT, необхідно вивчити детальні аспекти цієї атаки. Зловмисники інструктують свою армію ботнетів MIoT перезавантажити всі пристрої в певній або цільовій зоні покриття 5G одночасно, що викличе надмірні шкідливі запити, створюючи шкідливий сигнальний шторм. Використовуючи ці деталі, можна сформулювати вимоги до виявлення.

Компоненти 5G RAN, безпосередньо зазнавші цей тип атак, будуть найбільш ефективними елементами, які будуть відігравати важливу роль в процесі виявлення, з урахуванням необхідної реакції в реальному часі.. Відповідними компонентами 5G RAN NR або gNodeB є: радіопристрій (RU), модуль цифрової обробки радіосигналу в реальному масштабі часу (DU), і модуль цифрової обробки повільних процесів (CU). Враховуючи функції цих компонентів, ідеальним компонентом для виявлення цих типів атаки буде площина управління модулю цифрової обробки повільних процесів (CU-CP). Оскільки CU-CP відіграє важливу роль в управлінні протоколу керування

радіоресурсами (RRC), це було б найбільш ефективним місцем для впровадження функцій виявлення. Ключовими програмними елементами функцій виявлення, які повинні бути вбудовані в CU-CP, є аналітичні алгоритми для визначення того, чи є ця подія DDoS атакою. Функція аналітики також повинна мати можливість отримувати оновлення від зовнішньої платформи машинного навчання (ML) і штучного інтелекту (AI) за допомогою відкритих інтерфейсів.

3.4.9 Забезпечення безпеки в непублічній мережі

Для того, щоб вирішити проблеми безпеки в непублічній 5G мережі (NPN), необхідно відповідно до принципу нульової довіри (Zero-Trust Architecture, ZTA) забезпечити перевірку автентичності підключених до мережі пристроїв на кожному етапі, впровадивши федеративну модель ідентифікації та управління доступом (Federated Identity and Access Management, FIdAM).

Принцип ZTA полягає в підтримці безпеки навіть коли пристрій неконтрольовано, коли він рухається або знаходиться за межами периметра мережі. Федеративна модель ідентифікації - це підхід до безпеки 5G, який забезпечує єдину узгоджену архітектуру для перевірки автентичності, прав доступу, цілісності даних та інших компонентів і технологій в мережах 5g.

Такий підхід виключає можливість впровадити в мережу "роумінгову" вишку і перенаправити на неї захоплені SIM-карти. IT-системи зможуть повноцінно виявити підключення сторонніх пристроїв і блокувати паразитний трафік, що створює статистичний шум.

Для захисту SIM-карти від модифікації необхідно впровадити в неї додаткові засоби перевірки цілісності, можливо, реалізовані у вигляді SIM-додатків на базі блокчейна. Додаток може використовуватися для аутентифікації пристроїв і користувачів, а також для перевірки цілісності прошивки і налаштувань SIM-карти як в роумінгу, так і при роботі в домашній мережі.

Тобто рішення виявлених проблем з безпекою в непублічній 5G мережі можна представити в вигляді трьох підходів:

- впровадження федеративної моделі ідентифікації та управління доступом, яка забезпечить цілісність даних в мережі;
- забезпечення повної видимості загроз шляхом реалізації розподіленого реєстру для перевірки легітимності та цілісності SIM-карт;
- формування безмежної розподіленої системи безпеки, що вирішує питання взаємодії з пристроями в роумінгу.

Практична реалізація цих заходів вимагає часу і серйозних витрат.

3.5 Рекомендації по забезпеченню безпеки

Крім схвалення стандартів безпеки 3GPP, операторам необхідно розробити послідовну систему безпеки, яка стосується як і їх мережевого обладнання, так і їх управління мережею. Вона повинна охоплювати не тільки систему передачі даних, а й основні мережі та базові станції. Інші елементи мережі, такі як шлюзи для взаємозв'язку, брандмауери та IT-сервери (наприклад, DHCP, DNS та RADIUS), також повинні враховуватися в загальній системі безпеки. Застосовуючи цілісний підхід при розробці такої структури, оператори можуть гарантувати, що всередині мережі або на межі з іншими мережами не буде ніяких єдиних точок відмови. Безпека мереж 5G повинна бути розроблена як наскрізний (end-to-end) логічний рівень, що враховує специфіку кожного з наступних аспектів:

- Архітектури мережевої безпеки
- OAM (Операції, адміністрування та управління)
- Інтерфейсів на межі з зовнішніми мережами

Окрім архітектури мережевої безпеки, необхідний комплексний та безпечний набір правил, з якими оператори повинні дотримуватися керування рівня управління O&M (експлуатації та обслуговування). O&M має вирішальне значення для контролю ризиків всієї мережі. Тому для кожної задачі O&M слід застосовувати суворі правила безпеки. Сюди слід

віднести традиційні процедури, такі як управління конфігурацією обладнання та керування несправностями, а також більш вдосконалені функції, такі як нарізка мережі (slicing). Суворий адміністративний контроль, безумовно, є законною основою для надання прав доступу (серед варіантів, таких як читання / запис / копіювання / повний контроль) для фільтрації доступу до конфіденційної інформації.

Для того, щоб забезпечити швидкість роботи у віртуальній системі OAM, нові технології, такі як штучний інтелект (AI) / Машинне навчання (ML), володіють великим потенціалом для виявлення та аналізу загроз безпеці функціонування мережі. Альтернативою є NIST Cybersecurity Framework, яка може бути передовим досвідом для операторів для побудови системи управління стійкістю мереж.

Мережева безпека повинна постійно розвиватися для вирішення нових потенційних ризиків для безпеки, що виникають із відкритого Інтернету та розвитку нових сервісів. Власний або сторонній аудит безпеки або те і інше слід заохочувати як найкращу практику розширення можливостей мобільних мереж (не обмежуючись лише 5G). Оператори повинні бути пильними та завжди бути на крок попереду можливих загроз безпеці.

В порівнянні з попередніми бездротовими технологіями стандарти 5G включають в себе більше функцій безпеки для вирішення потенційних проблем безпеки і призводять до підвищення безпеки в майбутньому життєвому циклі 5G. Уряди можуть брати участь в цих зусиллях з контролю ризиків, пов'язаних з експлуатацією послуг 5G відповідно до нормативних актів країн. Рекомендована безпрограшна стратегія для вирішення проблеми безпеки 5G полягає в реалізації плану, описаного наступним чином:

- Формування нормативно-правових актів, що передбачають перехресну дискусію з усіма державними та приватними партнерами, щоб гарантувати послідовну систему безпеки. Уряди повинні взяти на себе ключову роль у визначенні потреб своїх відповідних країн з точки зору безпеки і заохочувати розробку нових технологій з механізмами контролю

ризиків для вирішення як своїх економічних завдань, так і потреб в області безпеки. Цього можна досягти завдяки співпраці з усіма зацікавленими сторонами на основі спільної мети визначення світових стандартів.

- Оператори повинні бути основним відповідальним органом за функціонування мережевої інфраструктури та здійснення управління ризиками відповідно до правил безпеки країни та офіційних стандартів органів. Крім того, уряди можуть проводити конкретну політику для забезпечення контролю за рівнем безпеки кожної мережі, що діє в країні.

Грунтуючись на успішному досвіді забезпечення безпеки 4G мереж, контроль ризиків безпеки 5G досягається спільними зусиллями всіх галузей промисловості. Щоб контролювати ризики в життєвому циклі 5G, необхідно постійно вдосконалювати рішення в області безпеки за допомогою технологічних інновацій і створювати безпечні системи і мережі за допомогою стандартів і екосистемного співробітництва

Постачальники обладнання: постачальники повинні робити свій внесок у роботі в галузі безпеки, дотримуватися стандартів та інтегрувати технології безпеки для створення безпечного обладнання. Разом з клієнтами та іншими зацікавленими сторонами, постачальники повинні забезпечити можливість підтримувати операторів для забезпечення безпечної роботи та кіберстійкості.

Оператори: оператори несуть відповідальність за безпечні операції та кіберстійкість власних мереж. Мережі 5G - це приватні мережі. Межі між різними мережами чітко зрозумілі. Оператори можуть запобігти зовнішнім атакам за допомогою брандмауерів та захисних шлюзів. Що стосується внутрішніх загроз, то оператори можуть керувати, контролювати і перевіряти всіх постачальників і партнерів, щоб переконатися в безпеці їх мережевих елементів.

Індустріальні та державні регулюючі органи: над стандартами безпеки необхідно всім спільно працювати. Це спільна відповідальність. З точки зору технологій, потрібно постійно вивчати ризики безпеки 5G в контексті (в

slicing, MEC, mMTC та інших сценаріях) та підвищувати безпеку засновану на протоколах (protocol-based). Що стосується забезпечення безпеки, необхідно стандартизувати вимоги до кібербезпеки та забезпечити, щоб ці стандарти були застосовні та піддавалися перевірці для всіх постачальників і операторів.

Для побудови системи, якій всі можуть довіряти, потрібні узгоджені обов'язки, уніфіковані стандарти та чітке регулювання.

Висновки до розділу: в даному розділі розглянуті та проаналізовані існуючі методи забезпечення безпеки, способи зменшення та протистояння загрозам, шляхи усунення існуючих та потенціально можливих вразливостей та представленно вдосконалені методи, а також власні рекомендації та ідеї для кращого забезпечення безпеки в мережах зв’язку 5G.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

5G використовуватиме мобільні хмари, SDN та NFV для вирішення завдань масового підключення, гнучкості та витрат. Маючи всі переваги, цим технологіям також властиві проблеми безпеки. Тому в даній бакалаврській роботі ми висвітлили основні проблеми безпеки, які можуть стати більш загрозливими для 5G, якщо їх не буде вирішено належним чином. Також представлено механізми безпеки та рішення цих проблем. Однак через обмежене автономне та інтегроване використання цих технологій у 5G, вектори загрози безпеці наразі не можуть бути повністю реалізовані. Аналогічно, проблеми безпеки та конфіденційності зв'язку будуть більш помітні, коли до 5G мереж буде підключено більше користувачів, наприклад пристрої Інтернету речей, і нові різноманітні набори послуг, які пропонуються в 5G. Підсумовуючи це, велика ймовірність, що поряд із впровадженням нових технологій та послуг 5G, виникнуть нові типи загроз та виклики безпеці. Однак врахування цих можливих загроз від початкових етапів проектування до розгортання самих мереж 5G зведе до мінімуму ймовірність можливих помилок безпеки та конфіденційності.

В результаті даної бакалаврської роботи представлено вдосконалені методи, а також написані рекомендації та пропозиції щодо забезпечення безпеки в 5G мережах. Для цього було розглянуто принцип роботи 5G мереж, поняття безпеки в цих мережах, а також проаналізовано архітектуру безпеки 5G мереж. В ході дослідження проаналізовано існуючі та можливі атаки, загрози, та вразливі місця в мережах п'ятого покоління, при цьому до уваги брались загрози пов'язані з Інтернетом речей, масовим IoT, загрози базової мережі, мережевого доступу, загрози віртуалізації, граничних обчислень, фізичної інфраструктури та загрози загального характеру. Також проведено аналіз загроз і вразливостей в непублічній 5G мережі, а також розглянуто можливі способи забезпечення безпеки в мережах 5G.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Правило В.В., Кормульов О.С. Методи забезпечення заданих показників безпеки // Збірник матеріалів XIV Міжнародної науково-технічної конференції "Перспективи телекомунікацій 2020". Київ: 2020. С. 178-180.

2. 5G EXPLAINED - HOW 5G WORKS // EMF Explained 2.0 URL: http://www.emfexplained.info/?ID=25916 (дата звернення: 07.06.2020).

3. Что такое 5G, и как сети пятого поколения изменят нашу жизнь // Tele2 URL: https://msk.tele2.ru/journal/article/what-is-5G (дата звернення: 07.06.2020).

4. Большие данные: архитектура сети и технологии 5G // Беспроводные технологии URL: https://wireless-e.ru/gsm/5g/big-data-5g/ (дата звернення: 07.06.2020).

5. 5G: everything you need to know // techradar URL: https://www.techradar.com/news/what-is-5g-everything-you-need-to-know (дата звернення: 07.06.2020).

6. Интернет вещей и 5G // Хабр URL: https://habr.com/ru/company/unet/blog/336936/ (дата звернення: 07.06.2020).

7. 5G: как работает технология и зачем нам это нужно // Rusbase URL: https://rb.ru/longread/what-is-5G/#rec142918336 (дата звернення: 07.06.2020).

8. БЕЗПЕКА ТА ЗАХИСТ БАЗ ДАНИХ // rusnauka URL: http://www.rusnauka.com/18_NPRT_2017/Informatica/4_227146.doc.htm (дата звернення: 07.06.2020).

9. Что такое информационная безопасность // Unotices URL: https://unotices.com/page-answer.php?id=14500 (дата звернення: 07.06.2020).

10. A guide to 5G network security // ericsson.com URL: https://www.ericsson.com/en/security/a-guide-to-5g-network-security (дата звернення: 07.06.2020).

11. Как защитить 5G от взлома: изучаем архитектуру безопасности // Хабр URL: https://habr.com/ru/company/trendmicro/blog/453120/ (дата звернення: 07.06.2020).

12. Введение в архитектуру безопасности 5G: NFV, ключи и 2 аутентификации // Хабр URL: https://habr.com/ru/post/481446/ (дата звернення: 07.06.2020).

13. Craig Gibson Securing 5G Through Cyber-Telecom Identity Federation // Trend Micro Research. 2019.

14. Уязвимости сетей 5G // Хабр URL: https://habr.com/ru/company/trendmicro/blog/486262/ (дата обращения: 07.06.2020).

15. Marco Lourenço, Louis Marinos, ENISA Threat assessment for the fifth generation of mobile telecommunications networks (5G) // ENISA THREAT LANDSCAPE FOR 5G NETWORKS. Листопад 2019.

16. 5G Americans The Evolution of Security in 5G // 5G Americans Whitepaper. Жовтень 2019.

17. 5G: НОВЫЕ ВЫЗОВЫ // business-magazine URL: https://business-magazine.online/fn_36738.html (дата звернення: 07.06.2020).

18. 5G security recommendations Package #1 // NGMN Alliance. 2016

19. Securing 5G Networks // Council on Foreign Relations URL: https://www.cfr.org/report/securing-5g-networks (дата звернення: 07.06.2020).

20. 5G Security White Paper // Huawei. 2019

21. Ijaz Ahmad. Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov 5G security: Analysis of threats and solutions // 2017 IEEE Conference on Standards for Communications and Networking (CSCN). Helsinki, Finland: 2017

22. A Comprehensive Guide to 5G Security / Madhusanka Liyanage ; Ijaz Ahmad ; Ahmed Bux Abro ; Andrei Gurtov ; Mika Ylianttila, 1st Edition вид. Helsinki, Finland: Kindle Edition, 2017.